Formes linéaires de logarithmes et équations Diophantiennes

Pagdame Tiebekabe

UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR
ÉCOLE DOCTORALE : MATHÉMATIQUES ET INFORMATIQUE
FACULTÉ DES SCIENCES ET TECHNIQUES

Année : 2022 **N° d'ordre :**

THÈSE DE DOCTORAT UNIQUE

Mention : Mathématiques et Modélisation

Spécialité : Codage, Cryptographie, Algèbre et Applications

Présentée par **Pagdame TIEBEKABE**

Soutenue le 22 février 2022

En vue de l'obtention du grade de

DOCTEUR DE L'UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

Titre de la thèse :
FORMES LINÉAIRES DE LOGARITHMES ET ÉQUATIONS DIOPHANTIENNES

Devant le jury

Président :	Hamidou DATHE	Professeur Titulaire	UCAD
Rapporteurs :	Maurice MIGNOTTE	Professeur Titulaire	Université de Strasbourg
	Omar KIHEL	Professeur Titulaire	Brock University
Examinateurs :	Mamadou SANGHARÉ	Professeur Titulaire	UCAD
	Oumar DIANKHA	Professeur Titulaire	UCAD
	Cheikh Thiécoumba GUEYE	Professeur Titulaire	UCAD
Directeur de thèse :	**Ismaïla DIOUF**	Maître de Conférences (CAMES)	UCAD

Année académique : 2021 - 2022

DÉCLARATION

Je soussigné Pagdame TIEBEKABE, déclare solennellement que la thèse intitulée **Formes linéaires de logarithmes et équations Diophantiennes** effectuée sous la direction du professeur Ismaïla DIOUF est basée sur notre propre travail et que nous avons explicitement indiqué tous les documents qui ont été utilisés.

Candidat : Pagdame TIEBEKABE **Directeur de thèse : Prof Ismaïla DIOUF**

PUBLICATIONS DE L'AUTEUR

1. P. Tiebekabe and I. Diouf, *Powers of Three as Difference of Two Fibonacci Numbers*, **JP Journal of Algebra, Number Theory & Applications**, Volume 49, Number 2, (2021), Pages 185 − 196. http ://dx.org/10.17654/NT049020185.

2. P. Tiebekabe and I. Diouf, *On solutions of the Diophantine equation* $L_n + L_m = 3^a$, **Malaya J. Mat.** $9(04)(2021), 228 - 238$. http ://doi.org/10.26637/mjm904/007.

3. P. Tiebekabe and I. Diouf, *On solutions of Diophantine equation* $F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a$, **Journal of Algebra and Related Topics**, Volume 9, Issue $2, 131 - 148(2021)$ https ://doi.org/10.22124/JART.2021.19294.1266.

4. P. Tiebekabe and I. Diouf. *Linear forms in logarithms and the mathematical method of diophantine equations : applications in chemistry and physics*. **J Math Chem** $59, 2009 - 2020(2021)$. https ://doi.org/10.1007/s10910-021-01274-y.

5. P. Tiebekabe and I. Diouf, *New Divisibility Tests*, **Far East Journal of Mathematical Education**, Volume 21, Number $1, (2021)$, Pages $31 - 41$. http ://dx.doi.org/10.17654/ME021010031.

6. P. Tiebekabe and S. Adonsou, *On Pillai's problem problem with Tribonacci and Pell-Lucas numbers*, **Indian Journal of Pure and Applied Mathematics**, (Springer 2021) | Submitted.

7. P. Tiebekabe, S. Adonsou and I. Diouf, *On Pillai's problem problem with Padovan and Pell-Lucas numbers*, **Khayyam Journal of Mathematics (KJM** 2021**)** | Submitted.

REMERCIEMENTS

Je remercie DIEU avant tout, de m'avoir donné la force et le courage d'accomplir ce modeste travail. La réalisation de cette thèse fut une occasion merveilleuse de rencontres et d'échanges avec de nombreuses personnes. Je ne saurais les citer toutes. Chacune à des degrés divers, mais avec une égale bienveillance, a apporté une contribution positive à sa finalisation. Mes dettes de reconnaissance sont, à ce point de vue, énormes à leur égard.

Je remercie particulièrement le professeur Ismaïla DIOUF, mon directeur de thèse, pour la finesse de ses attitudes sur le plan, aussi bien humain que scientifique. Ses remarques successives ont permis d'améliorer les différentes versions de ce travail. De lui, j'ai toujours reçu des encouragements et de précieux conseils pratiques. Grâce à son approche respectueuse de la personne humaine, je me suis continuellement senti à l'aise. Je lui en sais infiniment gré.

Je remercie également tous les enseignants de l'école doctorale de mathématiques et Informatique (EDMI) notamment les Professeurs Hamidou DATHE, Cheikh Thiécoumba GUEYE, Oumar DIANKHA et Mamadou SANGHARÉ pour leur accueil et leur bienveillance.

Je pense aussi aux professeurs Maurice MIGNOTTE et Omar KIHEL, qui se sont rendus disponibles pour instruire cette thèse.

J'ai une pensée très tendre à l'endroit de ma mère NAPALA Kuwèdaten que j'appelle affectueusement miss monde pour son apport quotidien à la réalisation de ce travail. Elle m'a toujours donné l'espoir d'aller de l'avant et partagé avec moi ma passion des mathématiques. Je suis très reconnaissant envers ma fiancée AGBEMAVI Ami Diane Innocente et de mon enfant Maxime. Innocente comme son nom, ma fiancée m'a été d'une aide incontestable surtout dans les moments difficiles de l'élaboration de cette thèse.

Je suis très reconnaissant à l'égard de la famille Diouf ainsi que leurs enfants pour leur amitié. Mes remerciements vont également à l'endroit de mes camarades doctorants du Laboratoire d'Algèbre, de Cryptologie, de Géométrie Algébrique et Applications (LACGAA), à mes amis à Dakar, à Lomé, à Kara et en France que je ne peux énumérer au risque d'en omettre certains. Enfin un grand merci à tous ceux qui ont contribué de près ou de loin à la réalisation de cette thèse.

DÉDICACES

Je dédie ce travail

À ma famille, particulièrement à mes feus parents Lardja TIEBEKABE et Kidibe KANGBENI, pour le goût à l'effort qu'ils ont suscité en moi, de par leur rigueur.

À toi ma mère Odile NAPALA, ceci est ma profonde gratitude pour ton éternel amour.

À mon fils Maxime.

Table des matières

INDICE DE NOTATION

$\mathbb{N}$	Ensemble des entiers naturels
$\mathbb{Z}$	Ensemble des entiers relatifs
$\mathbb{Q}$	Corps de nombres rationnels
$\mathbb{R}$	Corps de nombres réels
$\mathbb{C}$	Corps de nombres complexes
$n!$	$n \times (n-1) \times (n-2) \times \cdots 2 \times 1$
$\square$	Symbole marquant la fin d'une démonstration
L_n	n-ème nombre de Lucas
F_n	n-ème nombre de Fibonacci
$\mathcal{P}_n$	n-ème nombre de Padovan
P_n	n-ème nombre de Pell
$\mathcal{L}_n$	n-ème nombre de Pell-Lucas
$a\|b$	a divise b
pgcd (a,b)	Plus grand commun diviseur de a et b
ppcm (a,b)	Plus petit commun multiple de a et b
$\log(a)$	logarithme naturel
$\min(a,b)$	minimum de a et b
$\max(a,b)$	maximum de a et b
$a \equiv b \pmod{m}$	a est congru à b modulo m
$\Re(z)$	Partie réelle du nombre complexe z
$\|\|\alpha\|\|$	Distance de α à l'entier le plus proche
$A[x]$	Anneau de polynômes sur l'anneau intègre A
$\langle x_1, \cdots, x_n \rangle$	Idéal engendré par $x_1, \cdots, x_n$ éléments de l'anneau
$[\mathbb{K}_1 : \mathbb{K}_2]$	degré ou dimension du corps $\mathbb{K}_1$ sur le corps $\mathbb{K}_2$
G/H	H sous groupe normal de G
$\mathbb{Z}_p[u]$	$\{a + bu : a, b \in \mathbb{Z}\}$
$\mathbb{Z}[\frac{1}{p}]$	Anneau engendré par $\mathbb{Z}_p$ et $\frac{1}{p}$
$\|x\|$	Valeur absolue de x
$\lceil x \rceil$	Partie entière supérieure de x
$\lfloor x \rfloor$	Partie entière inférieure de x
$\lfloor x \rceil$	L'arrondi entier de x

$\mathcal{O}_{\mathbb{K}}$	Anneau des entiers algébriques de $\mathbb{K}$
$\binom{m}{n}$	Coefficient binomial
$v_p(a)$	valuation p-adique
$\|x\|_p$	norme p-adique
$c(P)$	Contenu d'un polynôme P
$\mathbb{Z}[i]$	Anneau des entiers de Gauss
$\mathbb{Z}[\sqrt{d}]$	Anneau engendré par $\sqrt{d}$
$\mathrm{Frac}(A)$	Corps de fractions de l'anneau A
$[a_0, a_1, \ldots, a_n]$	Fraction continuée de quotients $a_0, a_1, \ldots, a_n$
$H(\gamma)$	Hauteur naïve de γ
$h(\gamma)$	Hauteur logarithmique absolue de γ
$\mathbb{Z}/n\mathbb{Z}$	anneau quotient
$K[X]$	Anneau des polynômes à coefficients dans K
$(\mathbb{Z}/n\mathbb{Z})^*$	groupe des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$
$d_n(I)$	Sous-ensemble de l'anneau A constitué de 0 et des coefficients dominants des éléments de degré n de I
$fld_K(\gamma)$	Polynôme formel

INTRODUCTION

Le mot équation est l'un des termes mathématiques les plus connus de tous les mathématiciens ou non mathématiciens. Il construit un pont entre l'abstraction mathématique et la réalité physique. Nous savons que la plupart des phénomènes sont modélisés par des équations, non seulement différentielles mais aussi Diophantiennes. Considérons le problème suivant : dans l'enclos d'un zoo, cohabitent des tortues et des cigognes ; 14 pattes foulent le sol pour quatre animaux au total. Combien y a-t-il d'animaux de chaque espèce ? Le physicien Hideki Yukawa raconte dans son oeuvre autobiographique intitulée, *Le voyageur*, combien les instituteurs japonais prisaient ce type de petits problèmes dans le but de familiariser les jeunes écoliers avec l'arithmétique. Ceux-ci déterminaient la solution par une astuce qui se présente comme suit : si les quatre animaux, raisonnaient-ils, sont des tortues, cela fait 16 pattes au total ; 16 pattes qui sont réduites à 14 si l'une des tortues se met sur deux pattes. La solution est donc trois tortues et une cigogne. Yukawa trouvait ces solutions mystérieuses et préférait utiliser les bases d'algèbre que son goût précoce pour les mathématiques lui avait permis d'apprendre : si x est le nombre de tortues et y le nombre de cigognes, le problème revient à résoudre les deux équations suivantes :

$$4x + 2y = 14 \quad \text{et} \quad x + y = 4. \tag{1}$$

Sans savoir qu'elles se nomment ainsi, tous avons manipulé les équations Diophantiennes depuis notre enfance. Au fil du temps, celles-ci ont gagné en complexité et en abstraction. Certains d'entre nous ont eu à résoudre un problème de ce type : trouvez le rayon d'un cercle tel que la différence du périmètre d'un cercle et de sa surface soit égale au nombre π. Après simplification, ce problème revient à résoudre l'équation suivante :

$$x^2 - 2x + 1 = 0. \tag{2}$$

Les équations Diophantiennes sont des équations polynomiales à coefficients entiers où les inconnues sont des nombres entiers, comme :

$$x^2 + 5 = y^7 \quad \text{ou} \quad 4xyz + z^5 = x^2y^3. \tag{3}$$

Avec les méthodes générales dont nous disposons depuis une trentaine d'années, nous explorons année après année les arcanes des équations Diophantiennes.

Les équations Diophantiennes forment un vaste archipel dont l'exploration a commencé il y'a près de 2 000 ans. Îlot après îlot, les mathématiciens avancent sur ce territoire inhospitalier, mais fascinant.

Les équations Diophantiennes ont été nommées en l'honneur du mathématicien grec Diophantus d'Alexandrie encore appelé Diophante qui a consacré à ce type d'équations une série d'ouvrages.

Diophantus d'Alexandrie (né probablement entre 200 et 214 après JC ; mort vers l'âge de 84 ans, probablement entre 284 et 298) était un mathématicien alexandrin, auteur d'une série de livres intitulée Arithmetica, dont beaucoup sont maintenant perdus. Ses textes traitent de la résolution d'équations algébriques.

Les mathématiciens avaient principalement étudié l'arithmétique (addition, multiplication, puissance, etc.) et la géométrie. Diophante ouvre l'ère de l'algèbre et de ses équations.

Historiquement, le premier exemple d'équations Diophantiennes est probablement l'équation de Pythagore :

$$x^2 + y^2 = z^2 \tag{4}$$

qui consiste à trouver le triangle dont les côtés sont des entiers. Après Diophantus, d'éminents mathématiciens ont répondu à l'appel, soit pour formuler des conjectures comme celles de Pierre Fermat, de Catalan, etc., soit pour résoudre des problèmes (conjectures) comme celles d'Euler, de Gauss, de Lagrange, de Dedekind, etc. , afin de construire ce que nous avons aujourd'hui comme théorie des nombres.

La théorie des nombres est une branche des mathématiques qui se concentre principalement sur l'étude des nombres entiers positifs, ou nombres naturels, et de leurs propriétés telles que la divisibilité, la factorisation en nombres premiers ou la résolution des équations en nombres entiers. La théorie des nombres a une histoire très longue et diversifiée, et cer-

tains des plus grands mathématiciens de tous les temps, tels qu'Euclide, Euler et Gauss, y ont apporté une contribution significative. Tout au long de sa longue histoire, la théorie des nombres est souvent considérée comme la branche la plus pure des mathématiques car elle était loin de toute application spécifique. Cependant, des changements importants se sont produits au milieu des années 1970, et la théorie des nombres est maintenant devenue l'une des branches les plus importantes des mathématiques utilisées dans la cryptographie et l'échange sécurisé d'informations.

La résolution des équations Diophantiennes est un domaine de recherche à la fois ancien et d'actualité de la théorie des nombres. Les approches contemporaines de ces problèmes combinent généralement des méthodes issues de diverses branches des mathématiques fondamentales. Parmi celles-ci, les plus fructueuses reposent sur l'emploi de la théorie des formes linéaires de logarithmes associées à des résultats de modularité pour certaines représentations galoisiennes ou variétés abéliennes. Dans de nombreuses situations, l'obtention ou la qualité d'un tel résultat diophantien dépend crucialement de notre capacité à rendre effectifs les énoncés utilisés.

Beaucoup de chercheurs s'y sont intéressés d'une manière ou d'une autre, souvent, en utilisant ce puissant outil mis en place par Baker pour résoudre des problèmes jusqu'alors impossibles avec les techniques classiques.

Prenons le cas simple de la «conjecture de Catalan »résolue complètement en 2002 par Mihailescu. Les entiers 8 et 9 sont les seuls entiers naturels consécutifs qui sont des puissances entières d'entiers naturels. Même si Mihailescu a essayé de se passer de l'utilisation des formes linéaires de logarithmes, cela reste fondamental de voir comment ces dernières sont utilisées pour montrer que la question de Catalan

$$x^m - y^n = 1 \tag{5}$$

possède un nombre fini de solutions : résultat établi par Tijdeman en 1976. Immédiatement après la preuve de Tijdeman, Langevin donna un calcul effectif des bornes des solutions de l'équation de Catalan. Il a montré que

$$y^n, x^m < \exp^{\exp^{\exp^{\exp(730)}}}. \tag{6}$$

Une avancée considérable a été obtenue par Mignotte qui a prouvé que si p et q sont des

nombres premiers impairs et que l'équation

$$x^p - y^q = 1 \quad \text{possède une solution} \quad x, y \in \mathbb{N}, \quad \text{alors } \max\{p, q\} < 7.15 * 10^{11}. \tag{7}$$

Mignotte a aussi prouvé que :

$$\min\{p, q\} > 10^7. \tag{8}$$

Cette borne inférieure a été améliorée jusqu'à $3.2 * 10^8$ grâce à des calculs poussés effectués par Grantham et Wheeler.

La conjecture de Pillai est une généralisation naturelle du problème de Catalan.

Problème de Pillai

Subbayya Sivasankaranarayana Pillai (1901-1950) est un mathématicien indien spécialiste de la théorie des nombres. Il a écrit plusieurs articles sur les puissances parfaites. Une puissance parfaite est un nombre entier positif de la forme a^x où $a \geq 1$ et $x \geq 1$ sont des nombres entiers naturels. En 1931, S.S. Pillai a prouvé en [19] que pour tous entiers positifs a et b fixés, tous deux, le nombre de solutions (x, y) des inégalités Diophantiennes $0 < a^x - b^y \leq c$ est asymptotiquement égal à

$$\frac{(\log c)^2}{2(\log a)(\log b)}. \tag{9}$$

quand c tend vers l'infini. Il est très intéressant de lire la page 62 de cet article pour voir comment ce résultat a été obtenu. Ce résultat découle de la tentative de prouver que l'équation

$$m^x - n^y = a.$$

a seulement un nombre fini de solutions intégrales. Dans cette équation, m, n et a sont fixés. Les inconnus sont x et y. Après plusieurs années, il a repris cette même équation, mais, cette fois-ci, avec m, n, x et y comme inconnus en fixant seulement a.

Les recherches sur cette équation ont débuté avec S.S. Pillai en 1931. En 1936, A. Herschfeld ([17] et [18]) a poursuivi les recherches et a montré que si $|c|$ est un entier suffisamment grand, alors l'équation

$$2^x - 3^y = c \tag{10}$$

a au plus une solution (x, y) avec x et y des entiers positifs.

Ce résultat n'est plus vrai pour $|c|$ suffisamment petit. Par des méthodes classiques, Hersch-

feld a démontré que seuls les triplets d'entiers (x, y, c) avec x et y positifs tels que $2^x - 3^y = c$ est donné pour $|c| \leq 10$ par :

$$(2,1,1), (1,1,-1), (3,2,-1), (3,1,5), (5,3,5), (2,2,5), (4,2,7), (1,2,-7).$$

Donc si $x > 5$ ou $y > 3$, alors $|2^x - 3^y| > 10$. En procédant de la même manière, il a prouvé que si $x > 8$ ou $y > 5$, alors $|2^x - 3^y| > 100$.

S.S. Pillai ([17] et [18]) a étendu les résultats de Herschfeld au cas plus général des équations Diophantiennes exponentielles

$$a^x - b^y = c, \tag{11}$$

où a , b et c sont des entiers non nuls fixés avec $\text{pgcd}(a, b) = 1$ et $a > b \geq 2$. Il a montré qu'il existe un entier positif $c_0(a, b)$ tel que, pour $|c| > c_0(a, b)$, cette équation a au plus une solution. Cette preuve ne donne pas la valeur explicite de $c_0(a, b)$.

Dans le cas spécial de l'équation de Herschfeld avec $(a, b) = (2, 3)$, S.S. Pillai a conjecturé que $c_0(a, b) = 13$ et dit que l'entier c qui a deux représentations de la forme $3^n - 2^m$ sont les éléments de l'ensemble $\{-13, -5, 1\}$. Cette conjecture a été résolue par R. J. Stroeker et R. Tijdeman en 1982 par la mesure de l'indépendance linéaire des formes de logarithmes des nombres algébriques.

Conjecture 0.0.1 (Conjecture de Pillai)**.**
Pour tout entier $k \geq 1$, l'équation Diophantienne

$$x^n - y^m = k \tag{12}$$

admet un nombre fini de solutions entières positives (n, m, x, y), avec $n \geq 2$ et $m \geq 2$.

Depuis lors, plusieurs variantes de l'équation (11) ont été intensivement étudiées. Des résultats récents liés à l'équation $H_n - G_n = c$ où $(H_n)_{n\geq 0}$ et $(G_n)_{n\geq 0}$ représentent des suites récurrentes linéaires sont obtenus par M. Ddamulira et al dans lesquels ils ont résolu ce type d'équations de Pillai avec des nombres de Fibonacci et des puissances de 2 (voir [39]), M. Ddamulira et al ont résolu le cas avec des nombres de Fibonacci généralisés et des puissances de 2 (voir [40]), et Bravo et al ont résolu le cas des nombres de Tribonacci et puissances de 2 (voir [38]). Nous avons également résolu le cas des nombres de Padovan et des nombres de Pell-Lucas, en déterminant les nombres c qui ont au moins deux représentations comme

différence de nombres de Padovan et de Pell-Lucas. Plus simplement, nous avons résolu l'équation $\mathcal{P}_m - \mathcal{L}_n = c$ avec $m > 3$.

Numération de Zeckendorf

Édouard Zeckendorf (mathématicien Belge) a découvert dans [7] une propriété des nombres de Fibonacci qui débouche sur un système de numération. Il a énoncé et démontré le résultat suivant :

Théorème 0.0.1 (E. Zeckendorf)**.**
Pour tout entier naturel N, il existe une unique suite d'entiers $c_0, \ldots, c_k$ avec $c_0 \geq 2$ et $c_{i+1} > c_i + 1$, tels que

$$N = \sum_{i=0}^{k} F_{c_i},$$

où F_n est le n-ème nombre de Fibonacci.

En d'autres termes, tout entier positif s'écrit de manière unique comme une somme de nombres de Fibonacci d'indices plus grands que 1 et sont au moins distants de 1. C'est à cause de la condition initiale de la suite de Fibonacci qu'on demande que les indices de la décomposition soient plus grand que 1. Sans cela, la décomposition n'est pas assurée.

La décomposition d'un entier N est facile à obtenir : la suite de Fibonacci étant strictement croissante à partir du rang 2, il existe un entier $k \geq 2$ tel que

$$F_k \leq N \leq F_{k+1}.$$

On retient l'indice k. Si $N = F_k$, la décomposition est achevée. Sinon on recommence avec $N - F_k$. Par exemple, ce procédé fournit la décomposition suivante de 72.

$$72 = F_{10} + F_7 + F_4 + F_2.$$

Le système de numération associé est *la numération de Zeckendorf.*

Plusieurs cas particuliers de ce type d'équations ont été résolus. Par exemple, il y'a eu des recherches sur la détermination des puissances parfaites des suites de Fibonacci et Lucas. Le mérite revient à Bugeaud et al [37] qui, par des approches classiques et modulaires des équations Diophantiennes ont déterminé en 2006 toutes les puissances parfaites des suites

de Lucas et Fibonacci en résolvant les équations

$$F_n = y^p \quad \text{et} \quad L_n = y^p.$$

Premièrement, les puissances de 2 et plus tard les puissances parfaites des suites de Fibonacci et Lucas ont attiré l'attention des chercheurs. C'est dans ce sens que Bravo et Luca [25] ont déterminé en 2018 les puissances de 2 qui ont une représentation comme somme de deux nombres de Fibonacci. Deux ans plus tard F. Luca et V. Patel [28] ont généralisé en déterminant les puissances parfaites de la somme de deux nombres de Fibonacci. En 2015, J. Bravo et E. Bravo ont déterminé dans [26] les puissances de 2 qui ont une représentation comme somme de trois nombres de Fibonacci. Récemment, en 2021, [24], S. Kebli et al ont résolu l'équation

$$F_n \pm F_m = y^p.$$

D'autres problèmes sur les suites de Fibonacci et Lucas similaires à ceux discutés ont été étudié. Par exemple, des repdigits qui sont somme d'au plus trois nombres de Fibonacci ont été résolus [29] ; des repdigits qui sont somme de quatre nombres de Fibonacci ou Lucas ont été résolus dans [33] ; les nombres de Fibonacci qui sont somme de deux repdigits ont été obtenus dans [31] et des factorielles qui sont somme d'au plus trois nombres de Fibonacci ont été trouvées dans [30].

Notons que toutes ces équations ont été résolues grâce aux formes linéaires de logarithmes.

Cependant, il reste encore beaucoup d'équations Diophantiennes irrésolues à ce jour et nous nous proposons d'en résoudre quelques unes par les formes linéaires de logarithmes. Nous nous intéressons dans cette thèse à la détermination des puissances de 2 et 3 qui s'écrivent comme somme ou différence de certaines suites récurrentes linéaires (suites de Fibonacci et Lucas). Nous avons déterminé les puissances de 2 qui sont somme de quatre nombres de Fibonacci, les puissances de 3 qui sont somme de deux nombres de Lucas et les puissances de 3 qui sont différence de deux nombres de Fibonacci. Au-delà de ces résultats obtenus, nous avons aussi montré l'application de la méthode mathématique des équations Diophantiennes en Physique et en Chimie.

Cette thèse est structurée en trois chapitres.

Le premier chapitre développe les préliminaires sur les notions de bases en théorie des nombres et le deuxième chapitre traite des suites récurrentes linéaires et des équations Dio-

phantiennes. Quand au troisième chapitre, il traite des formes linéaires de logarithmes et leurs applications dans la résolution de plusieurs équations Diophantiennes exponentielles en suites récurrentes linéaires.

Chapitre 1

PRÉLIMINAIRES

Ce chapitre a pour but de discuter de quelques résultats importants en théorie des nombres. Ce sont des rappels sur les structures algébriques et arithmétiques. Nous faisons également des rappels sur les corps de nombres et leurs anneaux d'entiers. Ces notions sont importantes pour la compréhension chapitres suivants. La familiarité avec la définition et les propriétés de base des espaces vectoriels est supposée.

1.1 Définitions

1.1.1 Fractions continues

Définition 1.1.1.
Une fraction continue encore appelée fraction continue simple ou plus rarement fraction continuée, est une expression de la forme :

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + ...}}}}$$

comportant un nombre fini ou infini d'étages. On la note $[a_0, a_1, ..., a_n, ...]$.

Quand tous les a_i sont des entiers, la fraction continue est appelée fraction continue simple. Quand les a_i sont finis, elle se met sous la forme $[a_1, a_2, ..., a_k]$ et est appelée fraction continue simple finie. En utilisant la division euclidienne, nous pouvons développer tout nombre rationnel en fraction continue simple. Qu'en est-il des nombres irrationnels ? La réponse se trouve dans le théorème suivant.

Remarque 1.1.1. *Les cinq théorèmes suivants ont été énoncés et démontrés par I. Niven, H. S. Zuckerman, et H. L. Montgomery, dans leur livre intitulé* ***An introduction to the theory of number*** *en* 1991 *au Chapitre* 7 *pp* $325 - 359$.

Théorème 1.1.1.

Toute fraction continue simple infinie $[a_0, a_1, a_2, \cdots]$ *est un irrationnel.*

On note $[a_0, a_1, a_2, \cdots]$ la limite

$$\lim_{k \longrightarrow +\infty} [a_0, a_1, a_2, \cdots, a_k].$$

Pour tout k, $[a_0, a_1, a_2, \cdots, a_k]$ est un nombre rationnel $\frac{p_k}{q_k}$, appelée k ème réduite d'une fraction continue infinie et est obtenue par les expressions suivantes :

$$\begin{cases} p_{-2} &= 0, \\ p_{-1} &= 1, \\ p_i &= a_i p_{i-1} + p_{i-2} \quad \text{pour} \quad i \geqslant 0. \end{cases}$$

et

$$\begin{cases} q_{-2} &= 1, \\ q_{-1} &= 0, \\ q_i &= a_i q_{i-1} + q_{i-2} \quad \text{pour} \quad i \geqslant 0. \end{cases}$$

La réciproque du théorème 1.1.1 reste vraie comme le montre le résultat suivant.

Théorème 1.1.2.

Tout nombre irrationnel ξ *se développe uniquement en fraction continue simple infinie* $[a_0, a_1, a_2, \cdots]$, *où*

$$\begin{cases} a_i &= \lfloor \xi_i \rfloor, \\ \xi_{i+1} &= \dfrac{1}{\xi_i - a_i}. \end{cases}$$

avec $\xi_0 = \xi$

Pour la preuve, se référer au Théorème 7.10 de [5].

Le développement en fraction continue infinie $[a_0, a_1, a_2, \cdots]$ de ξ implique que la k ème réduite $\frac{p_k}{q_k}$ est l'approximation rationnelle de ξ. Le théorème suivant le montre.

Théorème 1.1.3.
Si a/b est un nombre rationnel avec $b \geqslant 1$ tel que $|\xi - \frac{a}{b}| < |\xi \times \frac{p_k}{q_k}|$, pour certains k, alors $b > q_k$.

En effet, si $|\xi b - a| < |\xi q_k - p_k|$ pour certains $k \geqslant 0$, alors $b \geqslant q_{k+1}$.

Plus généralement, nous avons le théorème suivant qui est très utile dans la détermination de la meilleure approximation rationnelle d'un nombre irrationnel.

Théorème 1.1.4 (Legendre)**.**
Soit ξ un nombre irrationnel. Si il existe un nombre rationnel a/b avec $b \geqslant 1$ tel que

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

alors a/b est égale à l'une des réduites dans le développement de ξ en fraction continue simple.

Discutons à présent du cas particulier où $\xi = \sqrt{m}$, où m est sans facteur carré.

Théorème 1.1.5.
Si l'entier positif m est sans facteur carré, le développement en fraction continue simple de $\sqrt{m}$ a la forme

$$\sqrt{m} = [a_0, \overline{a_1, ..., a_{r-1}, 2a_0}]$$

où $[a_0, \overline{a_1, ..., a_{r-1}, 2a_0}] = [a_0, a_1, ..., a_{r-1}, 2a_0, a_1, ..., a_{r-1}, 2a_0, \cdots]$ et r est appelée la longueur de la période de la fraction continue.

1.1.2 Triplet pythagoricien

Définition 1.1.2.
Un triplet pythagoricien ou triplet de Pythagore est un triplet (a, b, c) d'entiers naturels non nuls vérifiant la relation de Pythagore : $a^2 + b^2 = c^2$.

Le triplet pythagoricien le plus " simple" est $(3, 4, 5)$. Il est également le plus connu, ainsi que ses multiples : $(6, 8, 10)$, $(9, 12, 15)$ ...

Voici un théorème donnant une formule générant l'ensemble de ces triplets.

Théorème 1.1.6.

Le triplet (a, b, c) est pythagoricien si et seulement s'il existe deux entiers p et q, $0 < q < p$ tels que

$$\frac{a}{c} = \frac{p^2 - q^2}{p^2 + q^2} \quad et \quad \frac{b}{c} = \frac{2pq}{p^2 + q^2}.$$

La démonstration classique utilise une paramétrisation rationnelle du cercle unité :

Démonstration.

Il est possible de paramétrer le cercle unité d'équation $x^2 + y^2 = 1$, privé du point $A(-1, 0)$, à l'aide de la pente t de la droite passant par A et rencontrant le cercle en $M(x, y)$. Les coordonnées de M sont alors : $x = \frac{1 - t^2}{1 + t^2}$ et $y = \frac{2t}{1 + t^2}$. En effet, la pente de la droite (AM) étant t, on a $y = t(x + 1)$ et l'équation du cercle s'écrit alors $x^2 - 1 + t^2(x + 1)^2 = 0$ puis, après simplification par $x + 1$, non nul, et regroupement des termes, on obtient alors : $x = \frac{1 - t^2}{1 + t^2}$ puis $y = \frac{2t}{1 + t^2}$.

De plus, x et y sont des rationnels strictement positifs si et seulement si t est un rationnel strictement compris entre 0 et 1. Au triplet d'entiers strictement positifs (a, b, c), on associe le point M de coordonnées $(a/c, b/c)$ rationnelles strictement positives. Le triplet (a, b, c) est pythagoricien si et seulement si le point M est un point du cercle unité. Cela se traduit par les conditions :

$$\frac{a}{c} = x = \frac{1 - t^2}{1 + t^2} \quad \text{et} \quad \frac{b}{c} = y = \frac{2t}{1 + t^2}$$

où t est un rationnel q/p strictement compris entre 0 et 1. □

1.1.3 Groupes et Sous-groupes

Définition 1.1.3 (Groupe)**.**

Soit G un ensemble non vide et $* : G \times G \longrightarrow G, (a, b) \longmapsto a * b$ une application. $(G, *)$ est un groupe si :

a) $*$ est associative ie. $\forall a, b, c \in G, a * (b * c) = (a * b) * c$;

b) G possède un élément neutre e pour $*$ c'est-à-dire $\exists\, e \in G, \forall\, a \in G,\ a * e = e * a = a$;

c) tout $a \in G$ admet un symétrique ie. $\forall\, a \in G, \exists\, b \in G, a * b = b * a = e$.

Si, de plus, la loi $*$ est commutative i.e. $\forall\, a, b \in G,\ a * b = b * a$, alors on dit que G est un groupe commutatif ou abélien.

Exemple 1.1.1.

1. *$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ avec l'addition sont des groupes, de même que $\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ pour la multiplication.*
2. *Si E est un ensemble, l'ensemble $S(E)$ des bijections de E dans E, muni de la composition des applications est un groupe, appelé groupe symétrique de E. Si E n'a qu'un nombre fini n d'éléments, on note S_n le groupe symétrique de E et ses éléments sont appelés permutations.*

Définition 1.1.4 (Sous-groupe)**.**
Soit $H \subset G$ un sous-ensemble non vide. On dit que H est un sous-groupe de G si

i) $\forall a, b \in G, \quad a, b \in H \implies ab \in H$;

ii) $\forall a \in G, \quad a \in H \implies a^{-1} \in H$,

on notera $H < G$.

Les conditions *i)* et *ii)* sont évidemment équivalentes à l'unique condition

$$\forall a, b \in G, \quad a, b \in H \implies ab^{-1} \in H.$$

Définition 1.1.5 (Sous-groupe distingué)**.**
Un sous-groupe H de G est dit distingué (on note $H \lhd G$) si pour tout $g \in G, Hg = gH$ (On dit aussi invariant ou normal).

1.2 Anneaux

Définition 1.2.1 (Anneau)**.**
Un anneau $(A, +, \cdot)$ est la donnée d'un ensemble A et de deux lois internes $+, \cdot$ vérifiant :

- *$(A, +)$ est un groupe abélien.*
- *La multiplication $\cdot$ est associative et possède un élément neutre (noté 1).*
- *$\cdot$ est distributive par rapport à $+$: pour tous x, y, z dans A, on a $x \cdot (y + z) = x \cdot y + x \cdot z$ et $(y + z) \cdot x = y \cdot x + z \cdot x$.*

Si la multiplication est commutative, on dit que l'anneau A est *commutatif*.

Exemple 1.2.1.

1. *L'anneau nul* $\{0\}$.
2. $(\mathbb{Z}, +, \cdot), (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ *sont des anneaux commutatifs.*
3. *Un corps K est par définition un anneau commutatif, distinct de* $\{0\}$, *tel que tout élément non nul ait un inverse pour la multiplication.*
4. *Le produit direct* $\prod_{i \in I} A_i$ *d'une famille d'anneaux* $(A_i)_{i \in I}$ *est un anneau.*
5. *Si A est un anneau commutatif, on dispose de l'anneau des polynômes en n variables* $A[X_1, \cdots, X_n]$ *qui est commutatif.*

Définition 1.2.2.
On appelle ensemble des éléments inversibles d'un anneau A l'ensemble des $x \in A$ *tels qu'il existe* $y \in A$ *avec* $xy = yx = 1$. *C'est un groupe pour la multiplication, noté en général* A^*.

Exemple 1.2.2.

1. $(\mathbb{Z}/n\mathbb{Z})^*$ *est l'ensemble des classes* $\overline{m}$, *avec m premier à n.*
2. *Dans un corps K, on a par définition* $K^* = K \backslash \{0\}$.

Définition 1.2.3 (Homomorphisme)**.**
Un homomorphisme (ou morphisme) d'anneaux $f : A \longrightarrow B$ *est une application entre deux anneaux vérifiant :*

1. $f(x + y) = f(x) + f(y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

On notera que l'application nulle n'est pas un morphisme d'anneaux car elle ne vérifie pas la condition 3.

Définition 1.2.4 (Sous-anneau)**.**
Une partie A de B est un sous-anneau si $(B, +, \cdot)$ *est un anneau possédant le même élément unité que A.*

Il est équivalent de dire que $1 \in B$, et que $(B, +)$ est un sous-groupe de $(A, +)$ qui est stable par multiplication interne.

1.3 Idéaux, anneaux quotient

On supposera dans la suite que tous les anneaux sont commutatifs, sauf mention contraire.

Définition 1.3.1 (Idéal)**.**
Une partie I d'un anneau commutatif A est un idéal de A si elle vérifie :

- *I est un sous-groupe de A pour $+$.*
- *Pour tout x de I et tout a de A, on a $ax \in I$.*

On prendra garde de ne pas confondre cette notion avec celle de sous-anneau. En particulier un idéal de A contient 1 (ou encore un élément inversible de A) si et seulement s'il est égal à A.

Exemple 1.3.1.

1. *$\{0\}$ et A sont des idéaux de A. Ce sont les seuls si A est un corps.*
2. *Les idéaux de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n \in \mathbb{N}$.*
3. *Si E est une partie d'un anneau commutatif A, alors l'ensemble des éléments de A de la forme $a_1x_1 + \cdots + a_nx_n$ avec $x_i \in E$ et $a_i \in A$ est un idéal, appelé idéal engendré par E ; c'est le plus petit idéal de A contenant E. On notera $\langle a \rangle$ ou aA l'idéal engendré par un élément a de A.*

Proposition 1.3.1.
Soient A un anneau commutatif et I un idéal de A. Alors le groupe quotient A/I muni de la multiplication $\overline{a}\overline{b} := \overline{ab}$ est un anneau, appelé anneau quotient de A par I. La surjection canonique $p : A \longrightarrow A/I$ est un morphisme d'anneaux, et l'élément unité de A/I est $\overline{1}$.

Démonstration.
Le seul point non trivial est que l'élément $\overline{ab}$ de A/I ne dépend pas du choix des représentants a, b. Or si $\overline{a} = \overline{a}'$ et $\overline{b} = \overline{b}'$, alors il existe i, j dans I avec $a' = a + i, b' = b + j$ d'où $a'b' = ab + (aj + ib + ij)$ avec $(aj + ib + ij) \in I$. D'où $\overline{ab} = \overline{a'b'}$. □

On a donc immédiatement le théorème de factorisation habituel.

Définition 1.3.2.
Soit $f : A \longrightarrow B$ un morphisme d'anneaux. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A/\ker f \longrightarrow B$ tel que $f = \tilde{f} \circ p$, où $p : A \longrightarrow A/\ker f$ est la surjection canonique. De plus $\tilde{f}$ est injectif d'image $\operatorname{Im} f$, i.e. on a un morphisme d'anneaux $A/\ker f \backsimeq \operatorname{Im} f$.

Définition 1.3.3 (Anneau intègre)**.**
Un anneau commutatif A est dit intègre s'il est non nul, et si pour tous a, b de A, la condition $ab = 0$ implique $a = 0$ ou $b = 0$.

Exemple 1.3.2.

1. *Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est premier.*
2. *Tout corps est un anneau intègre.*
3. *Tout sous-anneau d'un anneau intègre est intègre.*
4. *Si A est intègre, les anneaux $A[X], A[X_1, \cdots, X_n]$ sont intègres.*

On rappelle le résultat classique suivant :

Proposition 1.3.2.
Soit A un anneau intègre, alors il existe un corps K et un homomorphisme injectif $i : A \longrightarrow K$ tel que pour tout morphisme injectif d'anneaux de A vers un corps K', il existe un unique morphisme de corps $j : K \longrightarrow K'$ tel que $f = j \circ i$. K est unique à isomorphisme près, et s'appelle le corps des fractions de A. On le note Frac A.

Cela signifie que K est le *plus petit corps* contenant A ; ainsi un anneau est intègre si et seulement s'il est sous-anneau d'un corps. Par exemple Frac $\mathbb{Z} = \mathbb{Q}$, et Frac $(K[X]) = K(X)$ (le corps des fractions rationnelles en une indéterminée). Noter que l'anneau nul n'a pas de corps des fractions (ce qui justifie qu'il ne soit pas intègre par convention).

Définition 1.3.4 (Anneau principal)**.**
Un anneau commutatif est dit principal s'il est intègre et si tous ses idéaux sont de la forme $\langle a \rangle = aA$ avec $a \in A$.

Par exemple $\mathbb{Z}$ et $K[X]$ (quand K est un corps) sont principaux.

Définition 1.3.5 (Idéal premier)**.**
Un idéal propre I de A est premier si et seulement si

$$\forall a, b \in A \quad [ab \in I \implies (a \in I \quad ou \quad b \in I)].$$

Exemple 1.3.3.

1. *Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $n\mathbb{Z}$ pour n premier.*
2. *Un anneau est intègre si et seulement si $\{0\}$ est premier.*
3. *L'image réciproque d'un idéal premier par un morphisme d'anneaux est un idéal premier.*

Définition 1.3.6 (Idéal maximal)**.**
Un idéal I de A est dit maximal si $I \neq A$ et si tout idéal J contenant I est égal à A ou à I.

Définition 1.3.7 (Idéal fractionnaire)**.**
Soit A un anneau intègre. Soit K le corps quotient de A. Un sous-ensemble non vide D de K vérifiant les trois propriétés suivantes :

- $\forall \alpha, \beta \in D, \alpha + \beta \in D$,
- $\forall \alpha \in D, \forall r \in A, r\alpha \in D$,
- *Il existe* $0 \neq \gamma \in A$ *tel que* $\gamma D \subset A$,

est appelé idéal fractionnaire de A.

Définition 1.3.8 (idéal intégral)**.**
Un idéal fractionnaire A est dit intégral lorsque $\gamma = 1$.

Définition 1.3.9 (Anneau intégralement clos)**.**
Un anneau intégralement clos est un anneau intègre A qui est sa propre clôture intégrale dans son corps des fractions. En d'autres termes, pour tout p et q non nuls appartenant à A, si p/q est racine d'un polynôme unitaire à coefficients dans A, alors p/q appartient à A.

Le théorème suivant est utile pour les questions théoriques générales.

Théorème 1.3.1 (Krull)**.**
Dans un anneau commutatif A, tout idéal $I \neq A$ est inclus dans un idéal maximal.

Démonstration.
L'ensemble des idéaux de A contenant I et distinct de A est inductif car si $(I_i)_{i\in I}$ est une famille totalement ordonnée d'idéaux de A distincts de A, la réunion est encore un idéal (parce que la famille est totalement ordonnée) distinct de A (parce qu'elle ne contient pas 1).

On applique alors le lemme de Zorn qui dit que tout ensemble inductif admet au moins un élément maximal. □

1.4 Divisibilité sur les anneaux intègres

1.4.1 Élément irréductibles, anneaux factoriels

Dans tout ce paragraphe, A désigne un anneau commutatif intègre.

Définition 1.4.1.
Soient a, b dans A. On dit que a divise b et on écrit $a|b$ s'il existe $c \in A$ tel que $b = ac$. En termes d'idéaux, c'est équivalent à $\langle a \rangle \supset \langle b \rangle$.

En particulier 0 ne divise que lui-même, et un élément de A^* divise tous les éléments de A.

Proposition 1.4.1.
Soient a, b dans A. Alors $(a|b \quad et \quad b|a)$ si et seulement s'il existe $u \in A^*$ tel que $a = ub$. On dit que a et b sont associés.

Démonstration.
Si $a = ub$ avec $a \in A^*$, alors $b|a$ et $b = u^{-1}a$ donc $a|b$. En sens inverse si $a = bc$ et $b = ad$ avec c, d dans A, alors $a = adc$ et donc $dc = 1$, soit $c \in A^*$. □

Définition 1.4.2.
On dit qu'un élément p de A est irréductible s'il vérifie les deux propriétés suivantes :

1. *p n'est pas inversible dans A.*
2. *La condition $p = ab$ avec a, b dans A implique que a ou b est inversible.*

La deuxième condition signifie que les seuls diviseurs de p sont ses associés et les inversibles de A. On fera bien attention au fait que par convention, les éléments de A^* ne sont pas irréductibles.

Par exemple, les irréductibles de $\mathbb{Z}$ sont les $\pm p$ avec p un nombre premier. Ceux de $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 sans racine réelle.

Définition 1.4.3 (Anneau factoriel)**.**
Un anneau commutatif A est dit factoriel s'il vérifie les trois propriétés suivantes :

1. *A est intègre.*

2. *Tout élément non nul a de A s'écrit comme produit*

$$a = up_1 \cdots p_r$$

avec $u \in A^*$ et les p_i irréductibles.

3. *Il y'a unicité de cette décomposition au sens suivant : si $a = vq_1 \cdots q_s$ en est une autre, alors $r = s$ et il existe une permutation σ de $\{1, \cdots, r\}$ telle que pour tout i de $\{1, \cdots, r\}$, les éléments p_i et $q_{\sigma(i)}$ soient associés.*

Pour ce qui est de la décomposition, on a besoin d'une propriété de finitude qui est à l'origine de la notion d'anneaux noethériens.

1.4.2 Anneaux noethériens

Dans tout ce paragraphe, A est un anneau commutatif, mais ici on ne suppose pas forcément que A est intègre.

Les propositions suivantes sont équivalentes.

Proposition 1.4.2.
Soit A un anneau commutatif.

1. *Tout idéal de A est engendré par un nombre fini d'éléments.*
2. *Toute suite croissante (pour l'inclusion) $(I_n)_{n\in\mathbb{N}^*}$ d'idéaux est stationnaire.*
3. *Toute famille non vide d'idéaux de A a un élément maximal pour l'inclusion.*

Définition 1.4.4 (Anneau noethérien)**.**
Un anneau commutatif A est dit noethérien s'il vérifie l'une des propositions précédentes.

Par exemple, tout anneau principal est noethérien, et si A est noethérien, tout quotient de A l'est encore. Par contre, l'anneau $K[(X_n)_{n\in\mathbb{N}^*}]$ n'est pas noethérien car $\langle X_1\rangle \subset \langle X_1, X_2\rangle \subset \cdots \subset \langle X_1, X_2, \cdots, X_n\rangle \subset \cdots$ forme une suite infinie strictement croissante d'idéaux.

Théorème 1.4.1 (Hilbert)**.**
Si A désigne un anneau noethérien, alors $A[X]$ est noethérien.

Démonstration.
Soient I un idéal de $A[X]$ et $n \in \mathbb{N}$; on note $d_n(I)$ le sous-ensemble de A constitué de 0 et des coefficients dominants des éléments de degré n de I. Il est immédiat que I est un idéal

de A, et que l'inclusion $I \subset J$ implique $d_n(I) \subset d_n(J)$. On a d'autre part les deux propriétés suivantes :

i) Si $n \in \mathbb{N}$, alors $d_n(I) \subset d_{n+1}(I)$: en effet il suffit de remarquer que si $P \in I$, alors $XP \in I$.

ii) Si $I \subset J$, alors le fait que $d_n(I) = d_n(J)$ pour tout $n \in \mathbb{N}$ implique que $I = J$: en effet si J contient strictement I, on choisit un polynôme Q de degré r qui a même coefficient dominant que P, mais alors $P - Q$ est dans $J \backslash I$ et est de degré $< r$, contradiction.

□

1.4.3 Critère de principalité et de factorialité

Dans ce paragraphe, A est de nouveau un anneau commutatif intègre.

Définition 1.4.5 (Anneau euclidien)**.**
L'anneau A est dit euclidien s'il existe une application $v : A\backslash\{0\} \longrightarrow \mathbb{N}$ («stathme euclidien») tel que si a, b sont non nuls dans A, alors il existe q, r dans A avec $a = qb + r$ et vérifiant : $r = 0$ ou $v(r) < v(b)$.

On ne demande pas d'unicité dans cette "division euclidienne". Par exemple, $\mathbb{Z}$ est euclidien avec $v(x) = |x|$, $K[X]$ (K corps) est euclidien avec $v(P) = \deg P$.

Théorème 1.4.2.
Si A est noethérien, alors A est principal.

Démonstration.
Soit I un idéal non nul de A, on choisit b non nul dans I avec $v(b)$ minimal. Alors tout a de I s'écrit $a = bq + r$ avec $r = 0$ ou $v(r) < v(b)$. Mais le deuxième cas est impossible car $r \in I$ d'où $a \in \langle b \rangle$. Finalement $I = \langle b \rangle$. □

La réciproque est fausse mais les contre-exemples classiques ne sont pas évidents ($\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$, $\mathbb{R}[X, Y]/X^2 + Y^2 + 1$).

Si A est principal, cela n'implique pas que $A[X]$ est principal (ceci n'est vrai que si A est un corps). Nous verrons que la propriété analogue est vraie pour factoriel. On commence par la définition du *contenu* d'un polynôme.

Définition 1.4.6.

Soit A un anneau factoriel. Le contenu (noté $c(P)$) d'un polynôme P est le pgcd de ses coefficients. P est dit primitif si $c(P) = 1$.

On notera que le contenu est défini à multiplication par un inversible de A près, par contre l'idéal qu'il engendre est bien défini.

Lemme 1.4.1 (Gauss)**.**

Pour tous P, Q de $A[X]$, on a $c(PQ) = c(P)c(Q)$ (toujours modulo A^*).

Démonstration.

Pour la preuve, on suppose premièrement que P et Q sont primitifs et on montre que PQ est primitif. P et Q étant positif, chacun a au moins un coefficient non divisible par p. On se ramène à P, Q primitifs en appliquant le résultat précédent à $P/c(P), Q/c(Q)$. □

On en déduit l'important résultat suivant :

Théorème 1.4.3.

Soit A un anneau factoriel de corps des fractions K. Alors les irréductibles de $A[X]$ sont de deux types

i) Les polynômes constants irréductibles dans A.

ii) Les polynômes primitifs de degré $\geqslant 1$ qui sont irréductibles dans $K[X]$.

En particulier, pour un polynôme primitif de $A[X]$, il revient au même d'être irréductible dans $A[X]$ et dans l'anneau principal $K[X]$ (ce qui n'est pas du tout évident étant donné qu'il y'a a priori plus de décompositions possibles dans $K[X]$).

Démonstration.

La démonstration de ce théorème est basée sur la "division euclidienne" et l'irréductibilité du polynôme P. □

On en déduit enfin le résultat suivant.

Théorème 1.4.4.

Si A est factoriel, $A[X]$ est factoriel.

Démonstration.

La preuve se fait en deux étapes. On montre d'abord qu'on a l'existence de la décomposition.

Ensuite on montre que si $P \in A[X]$ est irréductible, alors $\langle P \rangle$ est premier. □

Corollaire 1.4.1.

Si A est factoriel, $A[X_1, \cdots, X_n]$ est factoriel.

Il est commode d'avoir un critère pratique d'irréductibilité dans les anneaux factoriels. Le résultat suivant est souvent utile.

Théorème 1.4.5 (Critère d'Eisenstein)**.**

Soient A un anneau factoriel, P un polynôme non constant de $A[X]$, p irréductible dans A. On pose $P = \sum_{k=0}^{n} a_k X^k$ et on suppose :

1. *p ne divise pas a_n.*
2. *p divise a_k pour $0 \leqslant k \leqslant n-1$.*
3. *p^2 ne divise pas a_0.*

Alors P est irréductible dans $K[X]$(donc aussi dans $A[X]$ s'il est primitif).

Démonstration.

Pour des détails sur la preuve, se référer à la preuve du théorème 2.21 de [2]. □

1.5 Modules sur un anneau commutatif

La notion de module est la généralisation naturelle de celle d'espace vectoriel. Elle est absolument fondamentale, par exemple en géométrie algébrique et en théorie des nombres. Dans la suite, A est un anneau commutatif, que l'on sera amené à supposer non nul.

Définition 1.5.1 (Module)**.**

Un $A-$ module $(M, +, \cdot)$ est un ensemble muni d'une loi interne $+$ et d'une loi externe $\cdot : A \times M \longrightarrow M$ vérifiant :

$(\alpha, m) \longmapsto \alpha m$

- *$(M, +)$ est un groupe abélien.*
- *On a en plus quatre propriétés :*
  1. $\alpha(m + m') = \alpha m + \alpha m'$
  2. $(\alpha + \beta)m = \alpha m + \beta m$
  3. $(\alpha\beta)m = \alpha(\beta m)$

4. $1 \cdot m = m$

pour tous $\alpha, \beta \in A$ et tous $m, m' \in M$.

Remarque 1.5.1.

Comme A est supposé commutatif, il n'y a pas lieu de distinguer entre modules à gauche et à droite (pour A non commutatif, le troisième axiome serait différent pour un module à droite).

Définition 1.5.2 (Sous-module)**.**

Soit M un $A-$module. Un sous-module N de M est un sous-groupe de $(M, +)$ qui est en plus stable pour la multiplication externe de A.

Autrement dit une partie N de M est un sous-module si et seulement s'il contient 0, et si pour tous x, y de N et tout α de A on a : $x + y \in N$ et $\alpha x \in N$.

Définition 1.5.3.

Un homomorphisme (ou morphisme) de $A-$ modules est une application $f : M \longrightarrow M'$ entre deux $A-$ modules qui vérifie : $f(x+y) = f(x) + f(y)$ et $f(\alpha x) = \alpha f(x)$ pour tous x, y de M et tout α de A. On note $\ker f := f^{-1}(\{0\})$ le noyau de f et $\mathrm{Im}\, f := f(M)$ son image. Ce sont des sous-modules de M et M' respectivement.

Au lieu de morphisme de $A-$ modules, on dit parfois application $A-$linéaire. On a bien sûr les notions d'isomorphisme et d'automorphisme de $A-$modules.

La définition suivante est analogue à celle qu'on a dans les espaces vectoriels :

Définition 1.5.4.

- *Soit $(M_i)_{i \in I}$ une famille de $A-$ modules. La somme directe ("externe") des M_i est le sous module $\oplus_{i \in I} M_i$ du produit $\prod_{i \in I} M_i$ constitué des familles $(m_i)_{i \in I}$ presque nulles. Si I est fini, la somme directe coïncide avec le produit direct.*
- *Soit $(M_i)_{i \in I}$ une famille de sous-modules du A-module M. Alors le sous-module $\sum_{i \in I} M_i$ est le module engendré par la réunion des M_i. Si la condition $\sum_{i \in I} m_i$ implique $m_i = 0$ pour tout i (où $(m_i)_{i \in I}$ est une famille presque nulle avec $m_i \in M_i$ pour chaque i), on dit que la somme des M_i est directe ; dans ce cas $\sum_{i \in I} M_i$ est isomorphe à la somme directe $\oplus_{i \in I} M_i$, et on notera $\oplus_{i \in I} M_i$, pour $\sum_{i \in I} M_i$ ("somme directe interne").*

On notera que deux sous-modules M_1 et M_2 d'un A-module sont en somme directe si et seulement si $M_1 \cap M_2 = \{0\}$, mais ceci ne se généralise pas pour plus de deux sous-modules. D'autre part, si $M = M_1 \oplus M_2 = \{0\}$, alors M/M_1 est isomorphe à M_2 mais contrairement

au cas des espaces vectoriels, il n'y a pas de réciproque.

1.5.1 Module libres, modules de types fini

Définition 1.5.5 (Module de type fini)**.**
Un A-module M est dit de type fini s'il existe une partie finie S de M tel que M soit engendré par S.

Définition 1.5.6 (Module libre)**.**
Un module de type fini est dit libre s'il admet une base, i.e. une famille $(x_i)_{i\in I}$ telle que tout élément x de M s'écrive de manière unique $x = \sum_{i\in I} \alpha_i x_i$ avec $(\alpha_i)_{i\in I}$ famille presque nulle d'éléments de A.

1.6 Corps de nombres-Anneaux des entiers

Cette section est consacrée aux corps de nombres algébriques, aux entiers algébriques et aux propriétés importantes sur ces notions. Elle se termine par les propriétés et conditions de factorisation d'un idéal en produit d'idéaux premier. On montre également que cette décomposition est unique.

Définition 1.6.1 (Nombre algébrique)**.**
Un nombre algébrique est un nombre complexe solution d'une équation polynomiale à coefficients dans le corps $\mathbb{Q}$ des rationnels (autrement dit racine d'un polynôme non nul).

Exemple 1.6.1.
$\sqrt{2}, \sqrt{3}$ et $\sqrt{2}+\sqrt{3}$ sont des entiers de $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Définition 1.6.2 (Corps de nombres)**.**
Un corps de nombres algébriques (ou simplement corps de nombres) est une extension finie K du corps $\mathbb{Q}$ des nombres rationnels.

Cette définition signifie qu'un corps de nombres algébriques est un corps K qui est obtenu à partir du corps de nombres rationnels $\mathbb{Q}$ en adjoignant un nombre fini de nombres algébriques.

On notera d le degré d'un corps de nombres.

Exemple 1.6.2.
$\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{17})$ et $\mathbb{Q}(i, \theta)$, avec θ une racine du polynôme $x^3 + x + 1$ sont des corps de nombres.

Le théorème suivant appelé théorème de l'élément primitif montre qu'un corps de nombres

peut être obtenu en associant un seul nombre algébrique θ de $\mathbb{Q}$. Il s'agit du Théorème 6.1.1 démontré par S. Alaca et K. S.Williams dans [1].

Théorème 1.6.1.
Si K est un corps de nombres algébriques, alors il existe un seul nombre algébrique $\theta \in K$ tel que $K = \mathbb{Q}(\theta)$.

Pour un corps de nombres K de degré d, l'élément primitif a un polynôme minimal de degré d. Ce polynôme a alors d'autres racines $d-1$ (conjugués de l'élément primitif).

Définissons la notion de conjugué et de monomorphisme d'un corps de nombres algébriques.

Définition 1.6.3.
Soit $K = \mathbb{Q}(\theta)$ un corps de nombres algébriques de degré d. On appelle conjugué de θ sur $\mathbb{Q}$:

$$\theta_1 = \theta, \theta_2, \cdots, \theta_d$$

les racines du polynôme minimal de θ sur $\mathbb{Q}$.

Les corps $\mathbb{Q}(\theta_j)$ sont très similaires aux corps $\mathbb{Q}(\theta)$, où chacun est généré par un élément avec le même polynôme minimum f. En fait, ils sont tous isomorphes, d'après l'application $\sigma_j : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta_j)$ avec $\sigma_j(g(\theta)) = g(\theta_j)$, quand $g \in \mathbb{Q}[X]$. Nous avons le théorème 6.2.1 de [1] qui l'exprime.

Théorème 1.6.2.
Soit $K = \mathbb{Q}(\theta)$ le corps de nombres algébriques de degré d, alors on a exactement d monomorphismes distincts

$$\sigma_k : K \longrightarrow \mathbb{C} \quad avec \quad \sigma_k(\theta) = \theta_k \quad (k = 1, \cdots, d).$$

Exemple 1.6.3.
Soit $K = \mathbb{Q}(\sqrt{5})$. Alors $\sigma_1(x + y\sqrt{5}) = x + y\sqrt{5}, (x, y \in \mathbb{Q})$ et $\sigma_2(x + y\sqrt{5}) = x - y\sqrt{5}, (x, y \in \mathbb{Q})$ sont deux monomorphismes de K à $\mathbb{C}$.

Plus généralement, quand on a le corps $K = \mathbb{Q}(\theta)$ de nombres algébriques de degré d, pour tout γ élément de K, les conjugués de γ sur K sont $\gamma_1, \cdots, \gamma_d$ définis par

$$\gamma_1 = \sigma_1(\gamma), \cdots, \gamma_d = \sigma_d(\gamma)$$

où $\sigma_i, i = 1, 2, \cdots, d$ sont les monomorphismes définis précédemment.

Définition 1.6.4 (Polynôme formel sur un corps K)**.**
Soit K un corps de nombres algébriques de degré d. Soit $\gamma \in K$. Soit $\gamma_1 = \gamma, \gamma_2, \cdots, \gamma_d$ les $K-$ conjugués de γ. Alors le polynôme formel de γ sur K est le polynôme

$$fld_K(\gamma) = \prod_{i=1}^{d}(x - \gamma_k).$$

fld_K est un polynôme à coefficients dans $\mathbb{C}$ (ie. $fld_K(\gamma) \in \mathbb{C}[x]$). Le théorème 6.3.2 de [1] le prouve.

Théorème 1.6.3.
Soit K un corps de nombres algébrique de degré d. Soit $\gamma \in K$, alors

$$fld_K(\gamma) \in \mathbb{Q}[x].$$

On en déduit le corollaire suivant (Théorèmes 6.3.4 et 6.3.5 de [1]).

Corollaire 1.6.1.
Soit K un corps de nombres algébrique de degré d. Soit $\gamma \in K$. Nous avons les équivalences suivantes :

1. *Tous les K-conjugués de γ sont égaux si et seulement si $\gamma \in \mathbb{Q}$,*
2. *Tous les K-conjugués de γ sont distincts si et seulement si $K = \mathbb{Q}(\gamma)$.*

On a la caractérisation suivante des entiers algébriques en termes de modules qui est la Proposition 2.4 de [32].

Proposition 1.6.1.
Soit K un corps de nombres. Un élément γ de K est un entier algébrique si et seulement s'il existe un $\mathbb{Z}$-sous-module M de K non nul fini tel que $\gamma M \subset M$.

L'exemple 1.6.1 montre que la somme de deux entiers algébriques est aussi un entier algébrique. En réalité, l'ensemble des entiers algébriques a une structure d'anneau. Cela résulte de la Proposition 1.6.1. Nous avons le Théorème 2.1 de [32] qui a été démontré par J. S.Milne.

Théorème 1.6.4.

L'ensemble de tous les entiers (entiers algébriques) d'un corps de nombres K forme un anneau appelé anneau des entiers de K.

Nous donnons l'exemple intuitif suivant.

Exemple 1.6.4.

Pour $K = \mathbb{Q}$, nous avons $\mathcal{O}_K = \mathbb{Z}$.

Pour un corps quadratique de nombres (corps de nombres de degré 2). Ce n'est pas évident de déterminer son anneau des entiers. Nous avons le théorème suivant qui montre comment déterminer l'anneau des entiers. Il s'agit du Théorème 5.4.2 de [1].

Théorème 1.6.5.

Soit K un corps quadratique de nombres. Soit m le seul entier sans facteur carré tel que $K = \mathbb{Q}(\sqrt{m})$. Alors, l'ensemble $\mathcal{O}_K$ des entiers algébriques de K est donné par

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & m \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\dfrac{1+\sqrt{m}}{2}\right) & m \equiv 1 \pmod 4. \end{cases}$$

Lorsque K n'est pas un corps quadratique, il est plus difficile de déterminer $\mathcal{O}_K$. Déterminer $\mathcal{O}_K$ explicitement pour certaines classes de corps de nombres algébriques K est un domaine de recherche qui passionne certains chercheurs. Dans la section suivante, nous présenterons l'anneau de Dedekind et quelques propriétés.

1.6.1 Anneau de Dedekind

Pour résoudre des équations comme celle du dernier théorème de Fermat, l'anneau des entiers relatifs s'avère moins commode. Il est parfois plus simple de considérer d'autres anneaux, comme celui des entiers de Gauss, d'Eisenstein ou de Dirichlet. Le théorème des deux carrés de Fermat ou encore l'équation de Pell-Fermat illustre l'utilité d'une telle structure. Leurs études se fondent sur le cas particulier des entiers quadratiques, plus simple que le cas général.

Définition 1.6.5 (Anneau de Dedekind)**.**

Un anneau A est dit de Dedekind s'il vérifie les propriétés suivantes :

- *A est commutatif, unitaire, intégral,*

- *A est un anneau noethérien,*
- *A est intégralement clos,*
- *Chaque idéal premier non nul de A est maximal.*

Exemple 1.6.5.
Chaque anneau principal est un anneau de Dedekind. En particulier, il en va de même de l'anneau des entiers rationnels.

Théorème 1.6.6 (S. Alaca et K. S. Williams)**.**
Soit K un corps de nombres algébriques. Soit $\mathcal{O}_{\mathbb{K}}$ l'anneau des entiers de K. Alors, $\mathcal{O}_{\mathbb{K}}$ est un anneau de Dedekind.

Notez que chaque idéal fractionnaire A d'un anneau de Dedekind D est généré entièrement par un D sous-module de K. Nous pouvons définir la somme et le produit d'idéaux fractionnaires tout comme nous définissons la somme et le produit des sous-modules.

Théorème 1.6.7 (S. Alaca et K. S. Williams)**.**
Soit D un anneau intégral de corps quotient K et soit P un idéal premier de D. Alors, l'ensemble

$$\tilde{P} = \{\alpha \in K : \alpha P \subseteq D\}$$

est un idéal fractionnaire de D et il vérifie $\tilde{P}P = D$.

Exemple 1.6.6.
Considérons l'anneau de Dedekind $D = \mathcal{O}_{\mathbb{K}}$, où $K = \mathbb{Q}(\sqrt{6})$. L'ensemble

$$P = \langle 2, \sqrt{6} \rangle$$

est un idéal premier de D et $P = 2\mathbb{Z} + \mathbb{Z}\sqrt{6}$. Alors, on a

$$\tilde{P} = \frac{1}{2}P.$$

Le théorème précédent permet d'obtenir le théorème fondamental de l'anneau de Dedekind.

Théorème 1.6.8 (Théorème fondamental de l'anneau de Dedekind)**.**
Si D est un anneau de Dedekind, alors chaque idéal intégral est un produit d'idéaux premiers et cette

factorisation est unique en ce sens que si

$$P_1P_2\cdots P_k = Q_1Q_2\cdots Q_l,$$

où les P_i et Q_j sont des idéaux premiers, alors $k = l$ et après la réétiquetation (si nécessaire) $P_i = Q_i$, $i = 1, 2, \cdots, k$.

C'est l'équivalent du théorème fondamental de l'arithmétique.

Comme $\mathcal{O}_{\mathbb{K}}$ est un anneau de Dedekind, nous avons directement le résultat suivant :

Théorème 1.6.9 (S. Alaca et K. S. Williams)**.**
Soit K un corps de nombres algébriques. Alors, chaque idéal intégral premier de $\mathcal{O}_{\mathbb{K}}$ peut être exprimé uniquement comme un produit d'idéaux premiers.

Exemple 1.6.7.
Soit $K = \mathbb{Q}(\sqrt{-5})$, l'anneau des entiers $\mathcal{O}_{\mathbb{K}} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ de K est un anneau de Dedekind qu'on note D. D n'est pas un anneau de factorisation unique. En effet

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

où $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ sont irréductibles non associés de D. Nous montrons comment utiliser l'idéal pour restaurer la factorisation unique. Soit

$$P = \langle 2, 1 + \sqrt{-5}\rangle,$$
$$P_1 = \langle 3, 1 + \sqrt{-5}\rangle,$$
$$P_2 = \langle 2, 1 - \sqrt{-5}\rangle.$$

Alors

$$\langle 2\rangle = P^2, \quad \langle 3\rangle = P_1P_2, \quad \langle 1 + \sqrt{-5}\rangle = PP_1, \quad \langle 1 - \sqrt{-5}\rangle = PP_2$$

et

$$\langle 6\rangle = \langle 2\rangle\langle 3\rangle = \langle 1 + \sqrt{-5}\rangle\langle 1 - \sqrt{-5}\rangle = P^2P_1P_2.$$

La section suivante est dédiée aux logarithmes complexes et p-adiques.

1.7 Logarithmes Complexes et p-adiques

Dans cette section, nous abordons les notions de logarithmes complexes et p-adiques. Le logarithme est une fonction définie à priori sur $\mathbb{R}_+^*$, et nous l'étendons ici sur $\mathbb{C}$. On rappelle, pour la suite, que

$$\exp z = \sum_{n=0}^{+\infty} \frac{z^n}{n!} \quad \text{pour tout} \quad z \in \mathbb{C},$$

et pour

$$\arctan x = \sum_{n=0}^{+\infty} (-1)^n \frac{x^{2n+1}}{2n+1} \quad \text{pour tout} \quad x \in]-1,1[.$$

1.7.1 Logarithmes complexes

Écrivons tout d'abord la fonction ln sous forme de série. Nous savons que

$$\ln(1+t) = \sum_{n=0}^{+\infty} (-1)^n \frac{t^{n+1}}{n+1} \quad \text{pour} \quad |\, t \,| < 1;$$

On écrit donc

$$\ln\left(\frac{1+t}{1-t}\right) = 2\sum_{n=0}^{+\infty} \frac{t^{2n+1}}{2n+1}.$$

Si on pose $x = (1-t)/(1+t)$ alors $t = (x-1)/(x+1)$ et l'on a la proposition :

Proposition 1.7.1.
Pour $x > 1$, on a :

$$\ln x = 2\sum_{n=0}^{+\infty} \frac{1}{2n+1} \left(\frac{x-1}{x+1}\right)^{2n+1}.$$

Démonstration.
Posons $X = \dfrac{x-1}{x+1}$, alors on constate que si $x > 0$ alors $X \in]-1,1[$. Ainsi,

$$f(x) = 2\sum_{n=0}^{+\infty} \frac{1}{2n+1} \left(\frac{x-1}{x+1}\right)^{2n+1}$$

est bien définie et même dérivable sur $\mathbb{R}_+^*$ en vertu des théorèmes relatifs aux séries entières.

En dérivant, nous obtenons,

$$f'(x) = 2\sum_{n=0}^{+\infty} \frac{2}{(x+1)^2}\left(\frac{x-1}{x+1}\right)^{2n} = \frac{4}{(x+1)^2}\frac{1}{1-\left(\frac{x-1}{x+1}\right)^2} = \frac{1}{x}.$$

Donc ayant $f(1) = 0 = \ln 1$, on obtient bien $f(x) = \ln(x)$. □

Étendons ce résultat sur $\mathbb{C}$. Nous avons la proposition suivante :

Proposition 1.7.2.
On a pour tout $z \in \mathbb{C}_+$, avec $\mathbb{C}_+ = \{z \in \mathbb{C}/\mathcal{R}(z) > 0\}$,

$$\log_1 z = 2\sum_{n=0}^{+\infty} \frac{1}{(2n+1)}\left(\frac{z-1}{z+1}\right)$$

défini et dérivable pour $x \in \mathbb{R}_+^*$. On a $\log_1 x = \ln x$.

Démonstration.
Nous nous appuyons sur un résultat de la convergence normale sur tout compact de $\mathbb{C}_+$. Soit K un tel compact. On a la convergence dès que $\left|\frac{z-1}{z+1}\right| \leq r < 1$ (on s'appuie sur les résultats du logarithme dans $\mathbb{R}$).

En posant $z = x + iy$, on a

$$\left|\frac{z-1}{z+1}\right| = \frac{\sqrt{(x-1)^2+y^2}}{\sqrt{(x+1)^2+y^2}} = \sqrt{1 - \frac{(x+1)^2+y^2-y^2-(x-1)^2}{(x+1)^2+y^2}}$$

Donc

$$\left|\frac{z-1}{z+1}\right| = \sqrt{1 - \frac{4x}{(x+1)^2+y^2}}$$

or il est aisé de se rendre compte de la continuité de $\psi : z \in \mathbb{K} \longmapsto \frac{4x}{(x+1)^2+y^2}$ grâce à la continuité des applications (linéaires en dimension finie) et par composition d'applications continues. Ainsi, K étant compact, cette fonction atteint ses bornes et comme $\psi(z) > 0$, il existe $m > 0$ tel que $\psi(z) \geq m$ pour tout $z \in K$; donc

$$\left|\frac{z-1}{z+1}\right| \leq \sqrt{1-m} < 1,$$

d'où les résultats souhaités. □

Nous avons alors la proposition suivante :

Théorème 1.7.1.

Pour tout $z \in \mathbb{C}_+, \exp(\log_1 z) = z$

Démonstration.

Tout d'abord on démontre un lemme important : Pour tout couple de fonctions à variables réelles dérivables (f, g) on a : $\frac{g'}{g} = \frac{f'}{f} \Longrightarrow \exists c \in \mathbb{C}$ tel que $f = cg$.

Cela vient de la formule de la dérivée de la fonction rationnelle $\frac{f}{g}$. On fixe maintenant $x > 0$ et on pose

$$h(y) = 2\sum_{n=0}^{+\infty} \frac{1}{2n+1}\left(\frac{x+iy-1}{x+iy+1}\right)^{2n+1}.$$

Alors la série dérivée par rapport à y converge normalement sur tout compact de $\mathbb{R}$ (valable également sur $\mathbb{C}$ car avec $z = x + iy$, on retrouve la proposition précédente sachant qu'un produit de compacts est compact) h est dérivable sur $\mathbb{R}$ et $h'(y) = \frac{i}{x+iy}$. La fonction $g = \exp \circ h$ est dérivable, et on a $\frac{g'(y)}{g(y)} = \frac{i}{x+iy}$; en considérant que $y \longmapsto x + iy$ cette fonction et g ont même dérivée logarithmique (c'est-à-dire qu'elles vérifient les conditions du lemme) : il existe donc $c \in \mathbb{C}$ tel que $g(y) = c(x + iy)$. Or d'après la Proposition 1.7.1 on a $h(0) = \ln(x)$ et $c = 1$ puisque sur $\mathbb{R}_+^*$ on a bien $\exp(\ln(x)) = x$. □

Proposition 1.7.3.

Pour tout $z \in \mathbb{C}\backslash\mathbb{R}_-$ *il existe un unique* $a \in \mathbb{C}_+$ *tel que* $a^2 = z$*; on note* $a = \sqrt{z}$ *et si* $z = x + iy$ *on a :*

$$\sqrt{z} = \sqrt{\frac{x + \sqrt{x^2+y^2}}{2}} + i\frac{y}{\sqrt{2(x+\sqrt{x^2+y^2})}}.$$

Il suffit de le vérifier en calculant $\sqrt{z}^2$ et l'unicité provient du fait que $a^2 = b^2$. Ceci implique que $a = b$ ou $a = -b$. Vu que $\Re(a) > 0$, alors seul le cas $a = b$ est conservé.

On peut poser $\forall z \in \mathbb{C}\backslash\mathbb{R}_-$, $\ln z = 2\log_1(\sqrt{z})$. La proposition suivante étend les propriétés déjà vues pour ln.

Proposition 1.7.4.

- $\forall z \in \mathbb{C}\backslash\mathbb{R}_-, \quad \exp(\ln z) = z$

- $\forall z \in \mathbb{C}_+, \quad \ln z = \log_1 z$
- $\forall z \in \mathbb{C}\backslash\mathbb{R}_-, \quad \ln z = 2\ln(\sqrt{z})$

Démonstration.

- On a $\ln z = 2\log_1(\sqrt{z})$. Or $\sqrt{z} = \exp(\log_1(\sqrt{z}))$ d'après le théorème 2.3.1, $\exp(\ln z) = \exp(2\log_1(\sqrt{z}))$, et $\exp(\ln z) = (\exp(\log_1(\sqrt{z})))^2 = (\sqrt{z})^2 = z$
- Obtenu d'après le théorème 2.3.1,
- Obtenu avec la proposition ci-dessus.

En faisant le point, on se rend compte que le prolongement du logarithme sur $\mathbb{C}\backslash\mathbb{R}_-$ en fait toujours une application continue (grâce à la convergence normale de la Proposition 1.7.1 et 1.7.2 successivement). En étudiant les limites aux bornes, on peut se rendre compte que pour tout $\alpha < 0$ dans $\mathbb{R}$, on a $\lim_{z\to\alpha,\Re(z)>0} - \lim_{z\to\alpha,\Re(z)<0} \neq 0$; ce qui rend impossible un prolongement par continuité : notre prolongement de la fonction logarithme sur $\mathbb{C}$ est ici maximal. □

Ci-dessous deux autres propositions permettant d'éclaircir la fonction logarithme.

Proposition 1.7.5.
$\forall a \in \mathbb{R}_+$ *et* $\forall z \in \mathbb{C}_+$ *on a* $\ln(az) = \ln a + \ln z$

Démonstration.
Posons $z = x + iy$, a fixé. D'après le Théorème 1.7.1, on a :

$$\frac{\partial}{\partial y}(\ln a + \ln z) = \frac{i}{x+iy} = \frac{ai}{ax+aiy} = \frac{\partial}{\partial y}(\ln(az)).$$

Ayant les deux fonctions qui prennent la même valeur en 0 (on se ramène à $\ln(ax)$) et on se sert du cas réel pour obtenir le résultat souhaité. □

Passons à présent aux logarithmes $p-$adiques.

1.7.2 Logarithmes $p-$adiques

Définition 1.7.1 (Nombres $p-$adiques)**.**
Pour un nombre premier p fixé, les nombres $p-$adiques forment une extension particulière du corps $\mathbb{Q}$ des nombres rationnels, découverte par Kurt Hensel en 1897.

Le corps commutatif $\mathbb{Q}_p$ des nombres $p-$adiques peut être construit par complétion de $\mathbb{Q}$, d'une façon analogue à la construction des nombres réels par les suites de Cauchy, mais pour une valeur absolue moins familière, nommée valeur absolue $p-$adique.

Un nombre $p-$adique peut aussi se concevoir comme une suite de chiffres en base p, éventuellement infinie à gauche de la virgule (mais toujours finie à droite de la virgule), avec une addition et une multiplication qui se calculent comme pour les nombres décimaux usuels.

La principale motivation ayant donné naissance aux corps des nombres $p-$adiques était de pouvoir utiliser les techniques des séries entières en théorie des nombres, mais leur utilité dépasse à présent largement ce cadre. De plus, la valeur absolue $p-$adique sur le corps $\mathbb{Q}_p$ est une valeur absolue non archimédienne : on obtient sur ce corps une analyse différente de l'analyse usuelle sur les réels, que l'on appelle analyse $p-$adique.

Pour un nombre premier p donné, on définit comme suit la valeur absolue $p-$adique sur $\mathbb{Q}$.

- La valuation $p-$adique d'un entier relatif a non nul (notée $v_p(a)$) est l'exposant de p dans la décomposition de a en produit de facteurs premiers (il s'agit d'un cas particulier de valuation discrète). On pose $v_p(0) = +\infty$.
- On étend cette valuation à $\mathbb{Q}$ en posant :

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

  cette relation ne dépend pas du représentant choisi pour le rationnel.

- La valeur absolue $p-$adique $|\cdot|_p$ est définie par : $|r|_p = p^{-v_p(r)}$ (en particulier, $|0|_p = p^{-\infty} = 0$: en quelque sorte, plus r est divisible par p, plus sa valeur absolue $p-$adique est petite).
- Le corps $\mathbb{Q}_p$, muni d'une valeur absolue (encore notée $|\cdot|_p$, peut alors être défini comme le complété du corps valué $(\mathbb{Q}, |\cdot|_p)$.

1.7.2.1 Approche algébrique

Dans cette approche, on commence par définir l'anneau intègre $\mathbb{Z}_p$ des entiers $p-$adiques, puis on définit le corps $\mathbb{Q}_p$ des nombres $p-$adiques comme le corps des fractions de cet anneau.

On définit l'anneau $\mathbb{Z}_p$ comme la limite projective (qui est une généralisation du produit;

c'est le dual de la limite inductive) des anneaux $\mathbb{Z}/p^n\mathbb{Z}$, où le morphisme $\mathbb{Z}/p^{n+1}\mathbb{Z} \longrightarrow \mathbb{Z}/p^n\mathbb{Z}$ est la réduction modulo p^n. Un entier $p-$adique est une suite $(a_n)_{n\geq 1}$ telle que pour tout $n \geq 1$:

$$a_n \in \mathbb{Z}/p^n\mathbb{Z} \quad \text{et} \quad a_n \equiv a_{n+1} \pmod{p^n}.$$

Cet anneau est isomorphe à celui défini plus haut et l'est même en tant que anneau topologique, vu comme sous-anneau (compact) du produit des anneaux discrets $\mathbb{Z}/p^n\mathbb{Z}$. Le morphisme canonique de $\mathbb{Z}$ dans $\mathbb{Z}_p$ est injectif car 0 est le seul entier divisible par toutes les puissances de p.

Exemple, 7 étant un nombre $2-$adique, il correspond à la suite $(1,3,7,7,7,7,...)$. Toutes les suites (a_n) dont le premier élément n'est pas nul ont un inverse de $\mathbb{Z}_p$ car p est l'unique élément de l'anneau (c'est un anneau de valuation discrète) ; l'absence de cette propriété rendrait la même construction sans intérêt (algébrique) si l'on prenait pour p un nombre composé.

Exemple 1.7.1.
L'inverse de 7 dans $\mathbb{Z}_2$ est une suite qui commence par $1,3,7,7,23,55$ *(car* $7 \times 55 \equiv 1 \pmod{2^6}$*).*

On peut remarquer que $\mathbb{Z}_p$ contient donc l'anneau obtenu en adjoignant à $\mathbb{Z}$ tous les inverses des nombres premiers sauf p (ce sous-anneau est un anneau local, le localisé de $\mathbb{Z}$ en p). En effet, la localisation est une opération de base de l'algèbre commutative. Elle permet de construire à partir d'un anneau commutatif un nouvel anneau. La construction du corps de fractions est un cas particulier de la localisation.

De plus, p n'étant pas un diviseur de zéro dans $\mathbb{Z}_p$, le corps $\mathbb{Q}_p$ s'obtient en adjoignant simplement à l'anneau $\mathbb{Z}_p$ un inverse pour p, ce que l'on note $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$ (anneau engendré par $\mathbb{Z}_p$ et $\frac{1}{p}$, donnant les expressions polynomiales en $\frac{1}{p}$, analogue de la construction des nombres décimaux $\mathbb{D} = \mathbb{Z}\left[\frac{1}{10}\right]$).

1.7.2.2 Décomposition canonique de Hensel

D'après ce qui précède, tout élément non nul r de $\mathbb{Q}_p$ s'écrit de manière unique comme une série (automatiquement convergente pour la métrique $p-$adique) de la forme :

$$r = \sum_{i=k}^{\infty} b_i p^i$$

où k est un entier relatif et où les b_i sont des entiers compris entre 0 et $p-1$, b_k étant non nul. Cette écriture est la décomposition canonique de r comme nombre $p-$adique. Elle se déduit immédiatement du cas $r \in \mathbb{Z}_p$; c'est-à-dire $k \in \mathbb{N}$: si $r = (a_n) \in \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, la donnée des b_i équivaut à celle des a_n puisque

$$a_n \equiv \sum_{k \leq i < n} b_i p^i \pmod{p^n}.$$

On peut de cet fait représenter un entier $p-$adique par une suite infinie vers la gauche de chiffres en base p, tandis que les autres éléments de $\mathbb{Q}_p$, auront, quant à eux, en plus, un nombre fini de chiffres à droite de la virgule. Cette écriture fonctionne en somme à l'inverse de ce qu'on a l'habitude de rencontrer dans l'écriture des nombres réels. Par exemple, avec $p = 2$:

- $1 = 1 \times 2^0 = \ldots 000001_2 = 1_2$ (pour tout entier naturel, le développement $2-$adique est simplement le développement en base 2) ;
- $\ldots 111111_2 = \sum_{i=0}^{\infty} 2^i = -1$ (dans $\mathbb{Z}_2$, toute série géométrique de premier terme a et de raison 2 converge vers $\frac{a}{1-2} = -a$, car $|2|_2 = 2^{-1} < 1$) ;
- (vu que $|4|_2 = 2^{-2}$), alors $\ldots 01010101011_2 = 1 + \sum_{n=0}^{\infty} 2^{2n+1} = 1 + \frac{2}{1-4} = \frac{1}{3}$.

Le chapitre suivant aborde les notions de suites récurrentes linéaires et les équations Diophantiennes. Quelques propriétés et applications de ses suites sont présentées. La dernière partie analyse quelques méthodes classiques de résolution des équations Diophantiennes.

Chapitre 2

SUITES RÉCURRENTES LINÉAIRES ET ÉQUATIONS DIOPHANTIENNES

Ce chapitre aborde comme annoncé dans l'intitulé du chapitre, les suites récurrentes linéaires, les propriétés et relations entres elles. Ensuite, les différentes méthodes classiques de résolution des différentes équations Diophantiennes y sont analysées.

2.1 Suites récurrentes linéaires

2.1.1 Suites récurrentes linéaires d'ordre k

Définition 2.1.1.
Soit $k \geq 1$. La suite $(H_n)_{n\geq 0} \subseteq \mathbb{C}$ est appelée une suite récurrente linéaire d'ordre k si la suite

$$H_{n+k} = a_1 H_{n+k-1} + a_2 H_{n+k-2} + \cdots + a_k H_n \tag{2.1}$$

pour tout $n \geq 0$ avec $a_1, \ldots, a_k \in \mathbb{C}$, fixés.

On suppose que $a_k \neq 0$ (sinon, $(H_n)_{n\geq 0}$ est une suite récurrente d'ordre inférieur à k). Si on a $a_1, \ldots, a_k \in \mathbb{Z}$ et $H_0, \ldots, H_{k-1} \in \mathbb{Z}$, alors on peut aisément prouver par induction sur n que H_n est un entier pour tout $n \geq 0$. Le polynôme

$$f(X) = X^k - a_1 X^{k-1} - a_2 X^{k-2} - \cdots - a_k \in \mathbb{C}[X],$$

est appelé le polynôme caractéristique de $(H_n)_{n\geq 0}$. Supposons que

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i)^{\sigma_i}, \tag{2.2}$$

où $\alpha_1, \ldots, \alpha_m$ sont des zéros distincts de $f(X)$ avec respectivement $\sigma_1, \ldots, \sigma_m$ leur ordre de multiplicité.

2.1.2 Suites récurrentes binaires

Définition 2.1.2.

Les suites $(A_n)_{n\geq 0}$ et $(B_n)_{n\geq 0}$ sont définies pour tout entier positif par

$$\begin{cases} A_{n+2} &= aA_{n+1} + A_n, \quad A_0 = 0, \quad A_1 = 1 \\ B_{n+2} &= aB_{n+1} + B_n, \quad B_0 = 2, \quad B_1 = a. \end{cases}$$

Pour $a = 1$, $(A_n)_{n\geq 0} = (F_n)_{n\geq 0}$ et $(B_n)_{n\geq 0} = (L_n)_{n\geq 0}$, qui sont des suites de Fibonacci et Lucas respectivement, définies plus haut.

Remarque 2.1.1.

Si $k = 2$, la suite $(H_n)_{n\geq 0}$ est appelée suite récurrente binaire. Dans ce cas, le polynôme caractéristique est de la forme

$$f(X) = X^2 - a_1X - a_2 = (X - \alpha_1)(X - \alpha_2). \tag{2.3}$$

Supposons que $\alpha_1 \neq \alpha_2$, alors $H_n = c_1\alpha_1^n + c_2\alpha_2^n$ pour tout $n \geq 0$.

Définition 2.1.3.

La suite récurrente binaire $(H_n)_{n\geq 0}$ dont le terme général est donné par la formule (2.3) est dite non dégénérée si $c_1c_2\alpha_1\alpha_2 \neq 0$ et α_1/α_2 n'est pas un zéro de l'unité.

2.1.2.1 Cas particuliers des suites de Lucas

Les cas particuliers des suites de Lucas sont les suites de Fibonacci, de Lucas, de Pell et d'autres suites et nombres associés aux binômes.

(a) Soit $P = 1, Q = -1$, alors $D = 5$. Les nombres $U_n = U_n(1, -1)$ sont appelés les *nombres de Fibonacci*, tandis que les nombres $V_n = V_n(1, -1)$ sont appelés les *nombres de Lucas*. Voici les premiers nombres de Lucas : $2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 99, 322, \ldots$

(b) Soit $P = 2, Q = -1$, alors $D = 8$. Les nombres $U_n = U_n(2, -1)$ et $V_n = V_n(2, -1)$ sont les *nombres de Pell* et le *compagnon des nombres de Pell*. Voici quelques premiers termes de ces suites :

$U_n(2, -1) : 0, 1, 2, 5, 12, 29, 70, 169, \cdots$

$V_n(2,-1) : 2, 2, 6, 14, 34, 82, 198, 478, \cdots$

(c) Soient a et b des entiers tels que $a > b \geq 1$. Soient $P = a + b, Q = ab$, alors $D = (a-b)^2$. Pour tout $n \geq 0$, soit $U_n = \dfrac{a^n - b^n}{a-b}$ et $V_n = a^n + b^n$. Il est très facile de vérifier que $U_0 = 0, U_1 = 1, V_0 = 2, V_1 = a + b = P$, et $(U_n)_{n\geq 0}, (V_n)_{n\geq 0}$ sont la première et la seconde suite de Lucas de paramètres P, Q.

En particulier, si $b = 1$, on obtient les suites de nombres $U_n = \dfrac{a^n - 1}{a-1}, V_n = a^n + 1$; dans ce cas, les paramètres sont $P = a + 1, Q = a$. Finalement, si on a aussi $a = 2$, on obtient $U_n = 2^n - 1, V_n = 2^n + 1$, de paramètres $P = 3, Q = 2$.

2.1.3 Relations de récurrence

Une telle généralisation est possible lorsqu'on change les valeurs initiales, on mixe deux suites de Lucas tout en n'exigeant pas que les nombres dans la suite soient entiers, ou aient plus de deux paramètres.

Même si de nombreux résultats sur les suites de Lucas ont été étendus avec succès à des suites plus générales, et ont trouvé des applications intéressantes, nous choisissons dans cette section, de limiter notre attention uniquement aux suites de Lucas.

Soient P et Q des entiers. Soient T_0, T_1 des entiers tels que T_0 ou T_1 soient non nuls (pour exclure le cas trivial). Soit

$$W_0 = PT_0 + 2T_1 \quad \text{et} \quad W_1 = 2QT_0 + PT_1.$$

Soit

$$T_n = P \cdot T_{n-1} - Q \cdot T_{n-2} \quad \text{et} \quad W_n = P \cdot W_{n-1} - QW_{n-2} \quad (\text{pour} \quad n \geq 2).$$

Les suites $(T_n(P,Q))_{n\geq 0}$ et $(W_n(P,Q))_{n\geq 0}$ sont les (première et seconde) *suites linéaires de récurrence* de paramètres (P,Q) et *associée à la paire* (T_0, T_1). Les suites de Lucas sont spéciales, normalisées, suites linéaires de récurrence avec des paramètres donnés ; associées à $(0,1)$.

2.2 Quelques suites récurrentes linéaires

2.2.1 Suites de Fibonacci

La suite de Fibonacci est une suite d'entiers dans laquelle chaque terme est la somme des deux termes qui le précèdent. Elle commence par les termes 0 et 1 (il y'a aussi des définitions qui la font commencer avec 1 et 1). Les termes de cette suite sont appelés nombres de Fibonacci :

F_0	F_1	F_2	F_3	F_4	F_5	F_6	F_7	F_8	F_9	F_{10}	F_{11}	F_{12}	$\cdots$	F_n
0	1	1	2	3	5	8	13	21	34	55	89	144	$\cdots$	$F_{n-1}+F_{n-2}$

Elle est définie par $F_0 = 0$, $F_1 = 1$ et $F_n = F_{n-1} + F_{n-2}$ pour $n > 1$.

2.2.2 Expression fractionnelle

Le calcul du $n-$ème terme de la suite de Fibonacci via la formule de récurrence requiert le calcul des termes précédents. Au contraire, une expression fractionnelle de la suite de Fibonacci est une expression où le calcul du $n-$ème terme ne présuppose pas la connaissance des termes précédents. Binet a redécouvert une formule en 1843, qui avait déjà été obtenue par Moivre en 1718 et par Euler en 1765. Cette expression fractionnelle s'appelle la formule de Binet.

La formule de Binet pour le terme général des suites de Fibonacci et Lucas est obtenue en utilisant les techniques standards pour résoudre les suites récurrentes, qui sont données par :

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{et} \quad L_n = \alpha^n + \beta^n \tag{2.4}$$

où $\alpha = \dfrac{1+\sqrt{5}}{2}$ et $\beta = \dfrac{1-\sqrt{5}}{2}$ sont les zéros de l'équation caractéristique $X^2 - X - 1$. Cette suite est liée au nombre d'or α. Ce nombre intervient dans l'expression du terme général de la suite. Inversement, la suite de Fibonacci intervient dans l'écriture des réduites (convergents) de l'expression de α en fraction continue. Les quotients de deux termes consécutifs de la suite de Fibonacci sont les meilleures approximations du nombre d'or. Qu'en est-il des suites de Tribonacci ?

2.2.3 Suites de Tribonacci

La suite de Tribonacci est inspirée de **la suite de Fibonacci**. La suite de Tribonacci est définie par récurrence sur trois éléments. Chaque terme est la somme des trois précédents.

- $T_0 = 0\,; T_1 = 1\,; T_2 = 1$
- pour tout entier positif n, $T_{n+3} = T_{n+2} + T_{n+1} + T_n$.

Les premiers termes sont $0, 1, 1, 2, 4, 7, 13, 24, 44, 81$, etc.

Elle est la combinaison linéaire des trois suites (r_1^n) , (r_2^n) , (r_3^n) où les r_i sont les trois racines du polynôme : $x^3 - x^2 - x - 1$. La racine réelle, dont une valeur approchée est 1.8393, est appelée constante de Tribonacci (ou encore nombre d'argent, par référence au nombre d'or). Les racines complexes conjuguées ont un module inférieur à 1. Ils sont appelés aussi nombres de Tribonacci. Les termes de la suite de Tribonacci, sont parfois appelés entiers tribonacciques.

Il existe de même des suites de k-bonacci, où chaque terme est la somme des k termes précédents.

2.2.4 Suites de Lucas

Soient P et Q des entiers non nuls. Soit $D = P^2 - 4Q$, le *discriminant*, et supposons que $D \neq 0$ (pour exclure le cas dégénéré).

Considérons le polynôme $X^2 - PX + Q$, appelé *polynôme caractéristique*, qui a pour solutions

$$\alpha = \frac{P + \sqrt{D}}{2} \quad \text{et} \quad \beta = \frac{P - \sqrt{D}}{2}.$$

Donc $\alpha \neq \beta, \quad \alpha + \beta = P, \quad \alpha \cdot \beta = Q, \quad \text{et} \quad (\alpha - \beta)^2 = D.$

Pour tout $n \geq 0$, soient $U_n = U_n(P, Q)$ et $V_n = V_n(P, Q)$ tels que

$$U_0 = 0, U_1 = 1, U_n = P \cdot U_{n-1} - QU_{n-2} \quad (\text{pour} \quad n \geq 2),$$

$$V_0 = 2, V_1 = P, V_n = P \cdot V_{n-1} - QV_{n-2} \quad (\text{pour} \quad n \geq 2).$$

Les suites $U = (U_n(P, Q))_{n\geq 0}$ et $V = (V_n(P, Q))_{n\geq 0}$ sont appelées les (première et seconde) *suites de Lucas de paramètres* (P, Q). $V = (V_n(P, Q))_{n\geq 0}$ est encore appelée la *compagne* de la

suite de Lucas de paramètres (P, Q).

2.2.5 Développement en séries de puissances de $(U_n)_{n\geq 0}$ et $(V_n)_{\geq 0}$

Le développement en série de puissances formelles de $(U_n)_{n\geq 0}$ et $(V_n)_{\geq 0}$ pour tout (P, Q) se présente comme suit :

$$\sum_{n=0}^{\infty} U_n X^n = \frac{X}{1 - PX + QX^2} \quad \text{et} \quad \sum_{n=0}^{\infty} V_n X^n = \frac{2 - PX}{1 - PX + QX^2}. \tag{2.5}$$

En effet, les formules de Binet de $(U_n)_{n\geq 0}$ et $(V_n)_{\geq 0}$ sont données par les relations suivantes :

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{et} \quad V_n = \alpha^n + \beta^n.$$

Alors on a :

$$\begin{aligned}
\sum_{n=0}^{\infty} U_n X^n &= \frac{1}{\alpha - \beta}\left(\sum_{n=0}^{\infty}(\alpha X)^n - \sum_{n=0}^{\infty}(\beta X)^n\right) \\
&= \frac{1}{\alpha - \beta}\left(\frac{1}{1 - \alpha X} - \frac{1}{1 - \beta X}\right) \\
&= \frac{1}{\alpha - \beta} \times \frac{(\alpha - \beta)X}{1 - PX + QX^2} \\
&= \frac{X}{1 - PX + QX^2}.
\end{aligned}$$

De même,

$$\begin{aligned}
\sum_{n=0}^{\infty} V_n X^n &= \sum_{n=0}^{\infty}(\alpha^n + \beta^n) \\
&= \sum_{n=0}^{\infty}(\alpha X)^n + \sum_{n=0}^{\infty}(\beta X)^n = \frac{1}{1 - \alpha X} + \frac{1}{1 - \beta X} = \frac{2 - (\alpha + \beta)X}{1 - PX + QX^2} \\
&= \frac{2 - PX}{1 - PX + QX^2} \quad \text{car} \quad \alpha + \beta = P.
\end{aligned}$$

Les suites de Lucas sont des exemples de suites de nombres engendrés par un algorithme.

A la n$^{\text{ème}}$ étape ou au temps n, les nombres correspondants sont $U_n(P, Q)$, respectivement, $V_n(P, Q)$. Dans ce cas, l'algorithme est une récurrence linéaire avec deux paramètres. Une fois les paramètres et les valeurs initiales donnés, toute la suite, c'est-à-dire ses valeurs futures sont complètement déterminées. Mais, aussi, si les paramètres et deux valeurs consé-

cutives sont données, toutes les valeurs passées (et futures) sont déterminées.

2.2.6 Suites de Pell et Pell-Lucas

2.2.6.1 Suites de Pell

Définition 2.2.1.

Les suites de Pell sont des suites définies par la relation de récurrence suivante :

$$P_n = \begin{cases} 0 & pour \quad n = 0; \\ 1 & pour \quad n = 1; \\ 2P_{n-1} + P_{n-2} & pour \quad n \geq 2. \end{cases}$$

Les premiers nombres de Pell sont :

$$0, 1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, \cdots .$$

2.2.6.2 Propriétés des suites de Pell

Proposition 2.2.1.

Soit (P_n) la suite de Pell. On a les propriétés suivantes :

1. $P_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ *pour tout* $n \geq 0$ *avec* $\alpha = 1 + \sqrt{2}$ *et* $\beta = 1 - \sqrt{2}$,
2. $P_{n+1}P_{n-1} - P_n^2 = (-1)^n$ *pour tout* $n \geq 1$,
3. $\alpha^{n-2} \leq P_n \leq \alpha^{n-1}$ *pour tout* $n \geq 1$.

Démonstration.

1. Soient a et b deux nombres réels tels que $P_n - aP_{n-1} = b(P_{n-1} - aP_{n-2})$ alors $P_n = (a+b)P_{n-1} - abP_{n-2}$ par identification à la relation de récurrence $P_n = 2P_{n-1} - P_{n-2}$. On a $a + b = 2$ et $ab = -1$, donc $a = \alpha = 1 + \sqrt{2}$ et $b = \beta = 1 - \sqrt{2}$. Ainsi $P_n - \alpha P_{n-1} = \beta^{n-1}(P_1 - \alpha P_0) = \beta^{n-1}$. Alors $P_n = \alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \beta^{n-1}$, donc $P_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$.

2. En utilisant la formule établie, on obtient

$$\begin{aligned} P_{n+1}P_{n-1} - P_n^2 &= \frac{(\alpha^{n+1} - \beta^{n+1})(\alpha^{n-1} - \beta^{n-1})}{(\alpha-\beta)^2} - \frac{(\alpha^n - \beta^n)^2}{(\alpha-\beta)^2} \\ &= \frac{-\alpha^{n+1}\beta^{n-1} - \alpha^{n-1}\beta^{n+1} + 2\alpha^n\beta^n}{(\alpha-\beta)^2} \\ &= \frac{(-1)^n(\alpha^2 - 2\alpha\beta + \beta^2)}{(\alpha-\beta)^2} = (-1)^n. \end{aligned}$$

3. On sait que $P_n = \alpha^{n-1} + \alpha^{n-2}\beta + \cdots + \beta^{n-1}$ alors $P_n - \alpha^{n-1} = \alpha^{n-2}\beta + \cdots + \beta^{n-1}$, donc $P_n - \alpha^{n-1} = \beta P_{n-1} \leqslant 0$ pour tout $n > 1$, d'où $P_n \leqslant \alpha^{n-1}$.

   Sinon $P_n = \alpha^{n-1} + \alpha^{n-2}\beta + P_{n-2}\beta^2$. Donc

$$P_n - \alpha^{n-2} = \alpha^{n-1} - \alpha^{n-2}\beta + P_{n-2}\beta^2.$$

   Le signe du discriminant du polynôme en β dépend de $-1 + 2(\beta/\alpha)^{n-2}$ qui est négatif pour $n > 2$. Donc $P - n - \alpha^{n-2}$ a le signe de P_{n-2} qui est positif, alors $P_n \geqslant \alpha^{n-2}$, mais toujours vrai pour $n > 1$.

□

Remarque 2.2.1.

Ces relations peuvent être obtenues par induction sur n.

2.2.6.3 Suites de Pell-Lucas

Définition 2.2.2.

Les suites de Pell-Lucas sont des suites définies par la relation de récurrence suivante :

$$Q_n = \begin{cases} 2 & pour \quad n = 0; \\ 2 & pour \quad n = 1; \\ 2Q_{n-1} + Q_{n-2} & pour \quad n \geq 2. \end{cases}$$

Les premiers nombres de Pell-Lucas sont :

$$2, 2, 6, 14, 34, 82, 198, 478, 1154, 2786, 6726, 16238, 39202, \cdots .$$

On peut aussi écrire : $P_n = F_n(2)$ et $Q_n = L_n(2)$ où F_n et L_n sont respectivement les suites de

Fibonacci et de Lucas.

2.2.6.4 Propriétées des suites de Pell-Lucas

Proposition 2.2.2.

Soit $(Q_n)_{n\geq 0}$ la suite de Pell-Lucas

Les propriétés sont les suivantes :

1. $Q_n = \alpha^n + \beta^n$, *pour tout* $n \geq 0$ *avec* $\alpha = 1 + \sqrt{2}$ *et* $\beta = 1 - \sqrt{2}$,
2. $Q_{n+1}Q_{n-1} - Q_n^2 = 8(-1)^n$ *pour tout* $n \geq 1$,
3. $P_n Q_n = P_{2n}$.

Démonstration.

Idem que la dernière preuve. □

Présentons à présent les équations Diophantiennes.

2.3 Équations Diophantiennes

Dans cette section, nous allons dans un premier temps définir une équation Diophantienne et ensuite énumérer les différentes équations Diophantiennes existantes, puis nous discuterons de quelques cas particuliers d'équations Diophantiennes.

Définition 2.3.1.

Une équation Diophantienne est une équation polynomiale

$$f(x_1, x_2, \cdots, x_n) = 0, \tag{2.6}$$

à une ou plusieurs inconnues dont les solutions sont cherchées parmi les entiers, éventuellement rationnels, les coefficients étant eux-mêmes des entiers.

Exemple 2.3.1.

Trouver les couples (x, y) d'entiers tels que $x^4 = y^3 - 6$.

Trouver les solutions de cette équation n'est pas évident. Par contre, les outils de l'arithmétique élémentaire permettent de résoudre facilement les équations Diophantiennes linéaires encore appelées équations Diophantiennes de premier degré.

2.3.1 Équations Diophantiennes du premier degré

Définition 2.3.2.

On appelle équations Diophantiennes du premier degré, les équations Diophantiennes de la forme

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c, \tag{2.7}$$

où $a_1, a_2, \cdots, a_n$ sont des entiers.

Nous avons le théorème suivant sur l'existence de solutions pour les équations Diophantiennes de premier degré.

Théorème 2.3.1.

La condition nécessaire et suffisante pour que l'équation (2.7) admette une solution est que le plus grand commun diviseur de $a_1, a_2, \cdots, a_n$ divise c c'est-à-dire $pgcd(a_1, a_2, \cdots, a_n)|c$

Dans le cas de deux inconnus, nous avons le théorème suivant :

Théorème 2.3.2.

Si l'équation linéaire

$$ax + by = c \tag{2.8}$$

admet ξ et η comme solutions, alors toutes les solutions entières x et y de l'équation (2.8) se mettent sous la forme :

$$x = \xi + \frac{b}{pgcd(a,b)}t, \quad y = \eta - \frac{a}{pgcd(a,b)}t, \quad t \in \mathbb{Z}. \tag{2.9}$$

Démonstration.

Il est facile de voir que x et y données par les expressions (2.9) vérifient l'équation (2.8) quand nous considérons que $a\xi + b\eta = c$. Supposons que x, y sont des racines arbitraires intégrales de (2.8). Nous avons dans ce cas,

$$ax + by = c = a\xi + b\eta$$

Donc

$$a(x - \xi) = b(y - \eta). \tag{2.10}$$

Si $d = (a, b)$ le pgcd de a et b, il s'ensuit que $\frac{b}{d}$ est un diviseur de $x - \xi$. Par définition, il existe un entier t tel que $x - \xi = \frac{b}{d}t$.

Pour obtenir l'expression de y, il suffit de remplacer l'expression de $x - \xi$ obtenue précédemment dans l'équation (2.10). On obtient $y - \eta = -\frac{a}{d}t$. Donc, l'équation (2.8) a un nombre infini de solutions intégrales quand elle en admet. Une solution peut être obtenue par tâtonnement. □

L'algorithme d'Euclide permet également de trouver une solution fondamentale de (2.8). Sans perte de généralité, on peut poser $c = pgcd(a, b)$. On écrit l'algorithme sous la forme suivante :

$$\begin{cases} a - q_1 b & = & a_2 \\ b - q_2 a_2 & = & a_3. \\ \ldots\ldots\ldots & \ldots & \ldots \\ a_{r-3} - q_{r-2} a_{a_2} & = & a_{r-1} \\ a_{r-2} - q_{r-1} a_{a_1} & = & a_r = c \end{cases} \tag{2.11}$$

Éliminant a_{r-1} des deux dernières équations de (2.11), on obtient la relation

$$a_{r-2}(1 + q_{r-1}q_{r-2}) - q_{r-3}q_{r-1} = c.$$

En éliminant de la même manière a_{r-2} de cette équation et de la troisième équation du bas vers le haut du système (2.11), on obtient la relation suivante

$$a_{r-3}P + a_{r-4}Q = c,$$

où P et Q sont des entiers. En procédant de cette manière et en éliminant successivement a_{r-3}, a_{r-4}, etc., on obtient la relation $aA + bB = c$, où A et B sont des entiers déterminés par $q_1, q_2, q_3, \cdots, q_{r-1}$. Ceci peut être facilement vérifié par induction. Nous venons ainsi de trouver les solutions intégrales $x = A, y = B$ de l'équation (2.8).

Exemple 2.3.2.

Si $a = 15, b = 11, c = 1$, l'algorithme d'Euclide est

$$15 - 1 \cdot 11 = 4,$$
$$11 - 2 \cdot 4 = 3,$$
$$4 - 1 \cdot 3 = 1.$$

Par élimination, on obtient

$$4 \cdot 3 - 11 \cdot 1 = 1,$$
$$15 \cdot 3 - 11 \cdot 4 = 1.$$

et nous avons $x = 3$ *et* $y = -4$ *comme solution de l'équation* $15x + 11y = 1$.

Exemple 2.3.3.
Soient $a = 7$, $b = 12$ *et* $c = 5$. *L'algorithme d'Euclide permet de trouver* $\xi = -1$ *et* $\eta = 1$ *comme solution particulière. Comme pgcd(*a, b*)= pgcd (*$7, 12$*)=1, alors toutes les autres solutions sont* $x = -1 + 12t, \quad y = 1 + 7t, \quad t \in \mathbb{Z}$.

Abordons à présent les équations Diophantiennes non linéaires, celles dans lesquelles certaines inconnues figurent avec un degré supérieur ou égal à deux.

2.3.2 Équations Diophantiennes de second ordre

Dans cette section, nous allons définir et discuter des équations Diophantiennes de second ordre à deux inconnues. A travers les cas particuliers, nous allons étudier l'équation de Pythagore et sa généralisation à quatre inconnues.

Soit une équation Diophantienne de degré 2 à deux inconnues sous sa forme générale

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

Pour résoudre une équation Diophantienne de ce type, nous la mettons sous la forme suivante

$$Y^2 - DX^2 = N \quad \text{quand} \quad D \neq 0. \tag{2.12}$$

Pour ce faire, nous posons

$$X = 4ax + 2by + 2d, \quad Y = 2(4ac - b^2)y - (4ac - 2bd) \quad D = b^2 - 4ac$$
$$\text{et } N = (4ae - 2bd)^2 - 4(4ac - b^2)(4af - d^2).$$

Si $D < 0$, alors nous avons $Y^2 - N = DX^2 < 0$. Ce qui implique que $Y^2 < N$, d'où on a au plus un nombre fini de solutions. Par contre si D est un carré parfait, alors l'équation (2.12)

devient

$$Y^2 - X^2 = N. \tag{2.13}$$

En factorisant l'équation (2.13), nous obtenons

$$(Y + X)(Y - X) = N. \tag{2.14}$$

De cette équation, il s'en suit que $Y + X$ et $Y - X$ divisent N. Ceci implique que nous avons au plus un nombre fini de solutions. Pour résoudre l'équation (2.13), nous allons supposer que N est un carré parfait. Le problème consiste donc à déterminer le couple (X, Y) tel que (X, M, Y) soit un triplet pythagoricien avec $N = M^2$.

Dans la suite de cette section, nous donnerons quelques résultats sur l'équation de Pythagore et sa généralisation à quatre inconnues.

Théorème 2.3.3.

Les solutions intégrales de l'équation

$$x^2 + y^2 = z^2$$

sont données par

$$x = k(m^2 - n^2), \quad y = 2kmn, \quad z = k(m^2 + n^2) \quad avec \quad k, m, n \in \mathbb{Z}. \tag{2.15}$$

Plus généralement, nous avons le résultat suivant :

Théorème 2.3.4.

Toutes les solutions entières x, y, z, t avec y et z pairs de l'équation

$$x^2 + y^2 + z^2 = t^2$$

sont données par

$$x = \frac{l^2 + m^2 - n^2}{n}, \quad y = 2l, \quad z = 2m, \quad t = \frac{l^2 + m^2 + n^2}{n}$$

avec l et m des entiers positifs arbitraires et n un diviseur quelconque de $l^2 + m^2$.

Toutes les solutions sont obtenues exactement de cette façon.

Ce théorème résout un cas particulier d'une classe plus générale d'équations, qui est sous la forme

$$f(x) = 0,$$

avec $f(x) = \sum_{r,s=1}^{n} a_{rs}x_r x_s$ tel que $a_{rs} = a_{sr}$. Cette équation admet une solution (Théorème 1, Chapitre 7, [6]) si et seulement si $f(x) \equiv 0 \pmod{p}$ admet des solutions pour tous les nombres premiers p et entiers $r \geq 1$ avec pgcd$(x_1, x_2, \cdots, x_n, p)$=1.

Revenons à l'équation (2.13). D'après le Théorème 2.3.3, si N est impair, il n'y a pas de solution dans le cas contracté. On décompose $N/2$ en produit de 3 entiers et chacune des possibilités donne un triplet qui est solution de l'équation (2.13). Lorsque N est sans facteur carré, l'équation n'a pas de solutions ou possède un nombre fini de solutions.

Exemple 2.3.4.
Pour $x^2 - y^2 = 3$, on a $(2,1), (2,-1), (-2,1)$ et $(-2,-1)$ comme solutions. Mais l'équation $x^2 - y^2 = 6$ n'a pas de solution.

Considérons maintenant l'équation (2.12) lorsque D est sans facteur carré. Cette équation est appelée équation de Pell ou encore équation de Pell-Fermat.

2.3.2.1 Équation de Pell-Fermat

Définition 2.3.3.
L'équation de Pell-Fermat est une équation Diophantienne polynomiale quadratique. Si m est un entier positif qui est sans facteur carré et N un entier non nul, l'équation prend la forme suivante :

$$x^2 - my^2 = N. \tag{2.16}$$

Les solutions recherchées sont les solutions telles que y et x soient des entiers. Pour résoudre cette équation, on utilise les fractions continues. Il apparaît que certaines solutions des équations Diophantiennes quadratiques proviennent d'un k-ème convergent du développement en fraction continue.

Le théorème suivant donne la solution générale de l'équation 2.16.

Théorème 2.3.5.
Soit m un entier positif sans facteur carré et soit (h_k/k_k) la k ème réduite dans le développement de $\sqrt{m}$ en fraction continue simple. Soit N un entier vérifiant $|N| < \sqrt{m}$. Alors, toute solution positive $x = s, y = t$ de (2.16) avec pgcd$(s,t) = 1$ vérifie $s = p_k, t = q_k$, pour certains entiers positifs k.

Ce théorème implique que les solutions positives entières de l'équation $x^2 - my^2 = N$ sont

les numérateurs et dénominateurs d'une certaine k ème réduite de $\xi = \sqrt{m}$. Dans le cas où $N = \pm 1$, les solutions sont données par le théorème suivant.

Théorème 2.3.6.

Les solutions positives de $x^2 - my^2 = \pm 1$ sont trouvées parmi $x = p_k, y = q_k$, où p_k/q_k sont les réduites du développement de $\sqrt{m}$ en fraction continue simple. Soit r la période du développement de $\sqrt{m}$ en fraction continue.

- *Si r est pair, alors $x^2 - my^2 = -1$ n'a pas de solution. Toutes les solutions positives de $x^2 - my^2 = 1$ sont données par $x = p_{k_{r-1}}, y = q_{k_{r-1}}$ pour $k = 1, 2, 3, \cdots$.*
- *Si r est impair, alors $x = p_{k_{r-1}}, y = q_{k_{r-1}}$ donne toutes les solutions positives de $x^2 - my^2 = -1$ avec $k = 1, 3, 5 \cdots$ et toutes les solutions positives de $x^2 - my^2 = 1$ avec $k = 2, 4, 6, \cdots$.*

Remarque 2.3.1.

En d'autres termes, ce théorème montre que pour $N = 1$, l'équation de Pell a un nombre infini de solutions.

Considérons les ensembles $S = \{(a, b) \in \mathbb{N} \times \mathbb{N} : a^2 - mb^2 = 1\}$ et $T = \{a + b : a^2 - mb^2 = 1, (a, b) \in \mathbb{N} \times \mathbb{N}\}$.

Le théorème précédent implique que S est non vide. Vu qu'il existe une bijection entre T et S, le fait que S soit non vide implique que T qui est sous ensemble de $\mathbb{N}$ est aussi non vide. Par conséquent, T contient un plus petit élément. Soit (x_1, y_1) ce petit élément. Soit (x, y) une solution de l'équation $x^2 - my^2 = N$ de la forme $x + y\sqrt{m}$, nous avons le résultat suivant.

Théorème 2.3.7.

Si m est sans facteur carré, l'équation de Pell a un nombre infini de solutions $x + y\sqrt{m}$. Toutes les solutions positives entières sont obtenues grâce à la formule

$$x_n + y_n\sqrt{m} = \left(x_1 + y_1\sqrt{m}\right)^n$$

où $x_1 + y_1\sqrt{m}$ est la solution fondamentale de l'équation (2.16), avec $n \in \mathbb{N}$,

$$x_n = x_1^n + \sum_{k=1} \binom{2k}{n} x_1^{n-2k} y_1^{2k} m^k, \quad y_n = \sum_{k=1} \binom{2k-1}{n} x_1^{n-2k+1} y_1^{2k-1} m^{k-1}.$$

Ainsi, en utilisant le théorème 2.3.6, nous allons obtenir la solution fondamentale selon la parité de la longueur de la période du développement de $\sqrt{m}$ en fraction continue simple.

Le Théorème 11.6.1 de [1] donne la solution fondamentale.

Théorème 2.3.8.
Soit m un nombre entier positif sans facteur carré. Soit p_r/q_r $(r = 0, 1, 2, 3, \cdots)$ les réduites du développement de $\sqrt{m}$ en fraction continue infinie. Notons $\sqrt{m} = [a_0, \ldots, a_r, a_{r+1}, \ldots]$.

- *Si r est le premier indice tel que $a_{r+1} = 2a_0$, alors le développement de $\sqrt{m}$ est périodique à partir de ce dernier coefficient (i.e. la suite $a_1, \ldots, a_r$ se répète).*
- *Si r est impair (ce qui est le cas pour m=7), alors (p_r, q_r) fournit la plus petite solution de l'équation de Pell-Fermat $x^2 - my^2 = +1$; il n'y a pas de solution à l'équation $x^2 - dy^2 = -1$.*
- *Si r est pair (ce qui est le cas pour $m = 2$ ou 61), alors (p_r, q_r) fournit la plus petite solution de l'équation $x^2 - my^2 = -1$; la plus petite solution de l'équation de Pell-Fermat $x^2 - my^2 = +1$ est donnée par (p_{2r+1}, q_{2r+1}).*

Exemple 2.3.5.
Les développements en fraction continue de $x = \sqrt{2}$ et $y = \sqrt{7}$ s'écrivent respectivement

$$\sqrt{2} = [1, 2, 2, \ldots] \quad et \quad \sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \ldots].$$

On constate que les développements sont périodiques. Dans le cas de $\sqrt{2}$, la réduite initiale p_0/q_0 donne $p_0^2 - 2q_0^2 = -1$ et $p_1/q_1 = 3/2$ donne $p_1^2 - 2q_1^2 = +1$; dans le cas $\sqrt{7}$, la réduite $p_3/q_3 = 8/3$ donne $p_3^2 - 7q_3^2 = +1$. Le fait que le développement en fraction continue soit périodique est un cas particulier d'un théorème de Lagrange qui affirme que le développement en fraction continue du réel x est périodique si et seulement si x est quadratique, i.e. racine d'une équation à coefficient entiers de degré 2 (voir par exemple le livre de Hardy et Wright [4]).

Donnons un exemple illustrant la qualité de l'algorithme des fractions continues : la recherche de solutions de l'équation $x^2 - 61y^2 = 1$. Le développement en fraction continue de $x = \sqrt{61}$ s'écrit

$$\sqrt{61} = [7, 1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14, 1, \ldots],$$

et le développement devient périodique à partir de $a_{12} = a_1 = 1$. Les premières réduites sont $\frac{7}{1}, \frac{8}{1}, \frac{39}{5}, \frac{125}{16}, \frac{164}{21}, \frac{453}{58}, \frac{1070}{137}, \frac{1523}{195}, \frac{5639}{722}, \frac{24079}{3083}, \frac{29718}{3805}, \frac{440131}{56353}, \frac{469849}{60158}$.

La dixième réduite $p_{10}/q_{10} = 29718/3805$ fournit la première solution de l'équation $x^2 - 61y^2 = -1$. La solution fondamentale de $x^2 - 61y^2 = -1$ est dès lors fournit par

$x + y\sqrt{61} = (p_{10} + q_{10}\sqrt{61})^2$, *soit*

$$(x_1, y_1) = (1766319049,\ 226153980).$$

Exemple 2.3.6.

Considérons l'équation $x^2 - 7y^2 = 1$. *Le développement en fraction continue de* $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$, *la longueur de la période est* 4. *La longueur étant paire, alors la solution fondamentale est le numérateur et le dénominateur de la* 3 *ème réduite du développement de* $\sqrt{7}$ *en fraction continue, i.e* (p_3, q_3). *On a*

$$\frac{p_3}{q_3} = 2 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{1}}} = \frac{8}{3} \quad et \quad 8^2 - 7 \times 3^2 = 64 - 63 = 1.$$

Alors la solution générale de l'équation $x^2 - 7y^2 = 1$ *est*

$$x_n = 8^n + \sum_{k=1} \binom{2k}{n} 8^{n-2k} 3^{2k} 7^k, \quad y_n = \sum_{k=1} \binom{2k-1}{n} 8^{n-2k+1} 3^{2k-1} 7^{k-1}.$$

Nous avons donc montré que l'équation Diophantienne de la forme $f(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n = N$ avec f irréductible a un nombre infini de solutions si $n = 1, 2$. Si $n \geqslant 3$, alors l'équation précédente admet un nombre fini de solution. Ce résultat suivant prouvé par le mathématicien norvégien Axel Thue est une percée majeure dans la résolution de nombreuses équations Diophantiennes.

2.3.2.2 Équation de Thue

Dans cette section, nous discuterons du résultat de A. Thue qui donne la clé pour résoudre un nombre considérable d'équations Diophantiennes.

Théorème 2.3.9.

L'équation

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + \cdots + a_n y^n = m \neq 0 \tag{2.17}$$

où $n \geq 3$, *et* $f(x, y)$ *est irréductible sur* $\mathbb{Q}$, *a un nombre fini de solutions entières.*

Exemple 2.3.7.

Vu que le polynôme $t^3 - 2$ est irréductible sur $\mathbb{Q}$, alors l'équation Diophantienne

$$y^3 - 2x^2 = m \tag{2.18}$$

a un nombre fini de solutions. La preuve de l'existence de solutions entières finies de

$$f(x, y) = m > 0 \tag{2.19}$$

avec $f(x, y)$ un polynôme homogène de degré n irréductible sur $\mathbb{Q}$ donne une estimation du nombre de solutions. Cela n'aide cependant pas à trouver les solutions, car la méthode n'est pas constructive.

Baker a prouvé le résultat suivant :

Théorème 2.3.10.
Soit $t > n + 1$, alors les solutions de l'équation (2.19) vérifient l'inégalité

$$\max(|x|, |y|) < c \exp((\log m)^t),$$

où c est une constante effectivement calculable dépendant uniquement de n, et des coefficients de $f(x, y)$.

Exemple 2.3.8.
Soit $f(x, y) = x^3 - 2y^3$. Alors $|x| < M$, $|y| < M$ avec $M = (3 \times 10^5)^{23}$.

Passons à présent aux équations Diophantiennes de degré supérieur ou égal à 3.

2.3.3 Équations Diophantiennes de degré supérieur ou égal à 3

Dans cette section, nous considérerons des équations de degré supérieur ou égal à 3. Nous commençons par quelques équations de degré 4 résolues par la méthode de descente infinie de Fermat.

Théorème 2.3.11.
L'équation Diophantienne

$$x^4 - y^4 = z^2 \tag{2.20}$$

n'admet pas de solutions entières x, y et z.

Le dernier théorème implique que l'équation

$$x^4 + y^4 = 2z^2$$

n'a pas de solutions entières car elle peut être écrite sous la forme $z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2$.
Une variante de l'équation (2.18) à l'équation,

$$2x^4 - y^4 = z^2 \tag{2.21}$$

est une équation ayant une infinité de solutions d'après Nagell (Page 232, [3]). La preuve est basée sur la méthode de descente infinie généralisée.

S. Alaca et K. S.Williams ont démontré dans le Théorème 14.2.1, de [1] le résultat suivant qui est utilisé dans la résolution de l'équation de Mordell appelée ici équation de Bachet-Mordell (les équations de la forme $y^2 = x^3 + k$) puisque Bachet est celui qui a résolu le cas $k = 2$. Axel Thue a prouvé que ces équations ont de nombreuses solutions entières x et y.

Théorème 2.3.12.
Soit D un anneau de Dedekind. Soit A, B, C des idéaux intégraux de D tels que A et B soient premiers entre eux et

$$AB = C^n, \tag{2.22}$$

où n est un entier positif. Alors, il existe des idéaux A_1 et B_1 de D tels que :

$$A = A_1^n, \quad B = B_1^n, \quad C = A_1 B_1. \tag{2.23}$$

Le Théorème 14.2.3 dans [1] donne les conditions de résolutions de l'équation de Bachet Mordel $y^2 = x^3 + k$.

Théorème 2.3.13.
Soit k un entier tel que $k < -1$, k est sans facteur carré, $k \equiv 2, 3 \pmod 4$, $h(\mathbb{Q}(\sqrt{k})) \notin 3\mathbb{Z}$

- *S'il existe un entier a tel que $k = 1 - 3a^2$, alors les seules solutions entières de $y^2 = x^3 + k$ sont $x = 4a^2 - 1$ et $y = \pm(3a - 8a^3)$.*
- *Si $k = \pm 1 - 3a^2$, pour tout entier a, alors $y^2 = x^3 + k$ n'a pas de solutions entières x et y.*

Exemple 2.3.9.
L'entier $k = -2 = 1 - 3$ satisfait aux conditions du théorème précédent car $h(\mathbb{Q}(\sqrt{-2})) = 1$. Alors les seules solutions entières de l'équation $y^2 = x^3 - 2$ sont $(3, \pm 5)$. Ce résultat a été énoncé pour la première fois par Fermat.

Nous passons à l'analyse des équations Diophantiennes exponentielles.

2.3.4 Équations Diophantiennes exponentielles

Les équations Diophantiennes exponentielles sont les équations du type :

$$f(x_1^{m_1}, \cdots, x_n^{m_n}) = 0 \tag{2.24}$$

où f est un polynôme en n variables à coefficients entiers, dont les solutions sont les entiers positifs $(x_1, \ldots, x_n, m_1, \ldots, m_n)$.

Comme exemple d'équations classiques admettant des solutions par des factorisations en nombres entiers, nous pouvons citer :

$$x^2 + 1 = y^n$$

en (x, y, n), qui n'a pas de solution pour $n > 1$ et $y > 1$ (V. A. Lebesgues, 1850), et :

$$x^2 - 1 = y^n$$

qui n'a pas de solution pour $n > 1$ et $y > 3$ (Chao Ko, 1964).

Pour établir une conjecture de Ramanujan, l'équation :

$$x^2 + 7 = 2^n$$

n'a pour solutions que $n = 3, 4, 5, 7, 15$. Nagell (1960) a eu recours à la théorie algébrique des nombres (calculs dans le corps $\mathbb{Q}(\sqrt{-7})$. Les résultats de Alan Baker sur les formes linéaires de logarithmes ont permis de réaliser d'importants progrès (cf. nombres transcendants). Il s'agit en fait de méthodes d'approximation.

Ainsi, pour $f(x)$ un polynôme à coefficients entiers avec au moins deux zéros, on sait (A. Schinzel, R. Tijdeman, 1976) qu'il n'y a qu'un nombre fini d'entiers m pour lesquels l'équation :

$$y^m = f(x)$$

admet des solutions uniquement pour $y > 1$.

En général, la méthode de congruences est utilisée pour résoudre les équations Diophantiennes exponentielles mais elle devient difficile dans certaines situations. Il y a quelques outils liés à l'approche transcendantale pour résoudre les équations Diophantiennes exponentielles qui seront discutées dans le chapitre 3.

Il est important de présenter les différentes méthodes classiques de résolution des équations Diophantiennes. Ces méthodes permettent de résoudre beaucoup d'équations Diophantiennes. Cependant, elles sont limitées quand il s'agit de résoudre certaines équations Diophantiennes exponentielles. Face à ces dernières, on arrive à avoir quelques informations sur la nature des solutions. On peut soit montrer que l'équation admet des solutions ou pas, soit montrer que les solutions sont finies ou infinies sans pour autant les déterminer.

2.4 Méthodes classiques

Dans cette section, nous allons présenter quelques méthodes classiques de résolution des équations Diophantiennes. Nous donnerons des exemples dans chaque cas.

2.4.1 Méthode de factorisation

Soit à résoudre une équation de la forme $f(x_1, x_2, \cdots, x_n) = 0$. On réécrit cette équation dans sa forme équivalente suivante

$$f_1(x_1, x_2, \cdots, x_n) f_2(x_1, x_2, \cdots, x_n) ... f_k(x_1, x_2, \cdots, x_n) = a \tag{2.25}$$

avec $f_1, f_2, \ldots, f_k \in \mathbb{Z}[X_1, X_2, \cdots, X_n]$ et $a \in \mathbb{Z}$. En décomposant a en produit de facteurs premiers on obtient la décomposition de a en k facteurs premiers d'entiers $a_1, a_2, \cdots, a_k$.

Chacune de ses factorisations donne un système d'équations

$$\begin{cases} f_1(x_1, x_2, ..., x_n) &= a_1, \\ f_2(x_1, x_2, ..., x_n) &= a_2, \\ ..... &... \quad ... \\ f_k(x_1, x_2, ..., x_n) &= a_k. \end{cases}$$

La résolution de tous ces systèmes donne l'ensemble des solutions de l'équation (2.25). Nous allons illustrer cette méthode en présentant quelques exemples.

Exemple 2.4.1.

Déterminer toutes les solutions intégrales de l'équation

$$(x^2+1)(y^2+1) - 2(x-y)(1-xy) = 4(1+xy). \tag{2.26}$$

ou

$$(xy-1)^2 + (x-y)^2 - 2(x-y)(xy-1) = 4$$

Démonstration.

Cette équation est équivalente à

$$[xy - 1 - (x-y)]^2 = 4$$

ou

$$(x+1)(y-1) = \pm 2.$$

Si $(x+1)(y-1) = 2$, on obtient les systèmes d'équations suivant

$$\begin{cases} y-1 &= 2 \\ x+1 &= 1 \end{cases} \quad \begin{cases} y-1 &= -2 \\ x+1 &= -1 \end{cases} \quad \begin{cases} y-1 &= 1 \\ x+1 &= 2 \end{cases} \quad \begin{cases} y-1 &= -1 \\ x+1 &= -2 \end{cases}$$

ayant pour solutions $(1,2)$, $(-3,0)$, $(0,3)$, $(-2,-1)$.

Si $(x+1)(y-1) = -2$, on obtient les systèmes d'équations suivant

$$\begin{cases} y-1 &= -2 \\ x+1 &= 1 \end{cases} \quad \begin{cases} y-1 &= 2 \\ x+1 &= -1 \end{cases} \quad \begin{cases} y-1 &= -1 \\ x+1 &= 2 \end{cases} \quad \begin{cases} y-1 &= 1 \\ x+1 &= -2 \end{cases}$$

ayant pour solutions $(1,0)$, $(-3,2)$, $(0,-1)$, $(-2,3)$. □

Toutes les huit paires trouvées satisfont à l'équation (2.26).

Exemple 2.4.2.

Soient p et q des nombres premiers. Trouver les solutions entières de l'équation

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{pq}.$$

Démonstration.

Cette équation peut se réécrire de la façon suivante :

$$(x-pq)(y-pq)=p^2q^2.$$

Comme $\frac{1}{x}<\frac{1}{pq}$ alors $x>pq$.

Considérant tous les diviseurs de p^2q^2, on a les systèmes suivants

$$\begin{cases} x-pq &= 1 \\ y-pq &= p^2q^2 \end{cases}, \quad \begin{cases} x-pq &= p \\ y-pq &= pq^2 \end{cases}, \quad \begin{cases} x-pq &= q \\ y-pq &= p^2q \end{cases},$$

$$\begin{cases} x-pq &= p^2 \\ y-pq &= q^2 \end{cases}, \quad \begin{cases} x-pq &= pq \\ y-pq &= pq \end{cases}, \quad \begin{cases} x-pq &= pq^2 \\ y-pq &= p \end{cases},$$

$$\begin{cases} x-pq &= p^2q \\ y-pq &= q \end{cases}, \quad \begin{cases} x-pq &= q^2 \\ y-pq &= p^2 \end{cases}, \quad \begin{cases} x-pq &= p^2q^2 \\ y-pq &= 1 \end{cases}.$$

Les solutions de ces systèmes sont

$$\begin{gathered}(1+pq,pq(1+pq)),\quad (p(1+q),pq(1+q)),\quad (q(1+p),pq(1+p)),\\ (p(p+q),q(p+q)),\quad (2pq,2pq),\quad (pq(1+q),p(1+q)),\\ (pq(1+p),q(1+p)),\quad (q(p+q),p(p+q)),\quad (pq(1+pq),1+pq).\end{gathered}$$

□

Remarque 2.4.1.

L'équation

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n}$$

où $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ a $(2\alpha_1+1)\cdots(2\alpha_k+1)$ comme solutions positives entières.

En effet, l'équation est équivalente à :

$$(x-n)(y-n) = n^2,$$

et $n^2 = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ a $(2\alpha_1+1)\cdots(2\alpha_k+1)$ comme diviseurs positifs .

Exemple 2.4.3.

Déterminer toutes les solutions positives (x,y) pour lesquelles

$$(xy-7)^2 = x^2+y^2.$$

Démonstration.

L'équation équivalente est

$$(xy-6)^2 + 13 = (x+y)^2$$

ou

$$(xy-6)^2 - (x+y)^2 = -13.$$

Après factorisation, on obtient l'équation suivante

$$[xy-6-(x+y)][xy-6+(x+y)] = -13,$$

donnant les systèmes suivants :

$$\begin{cases} xy-6-(x+y) &= -1 \\ xy-6+(x+y) &= 13 \end{cases}, \quad \begin{cases} xy-6-(x+y) &= -13 \\ xy-6+(x+y) &= 1. \end{cases}$$

Après réduction, on a les systèmes équivalents suivants :

$$\begin{cases} x+y &= 7 \\ xy &= 12 \end{cases}, \quad \begin{cases} x+y &= 7 \\ xy &= 0. \end{cases}$$

qui ont pour solution $(3,4),(4,3),(0,7),(7,0)$. □

Exemple 2.4.4.

Trouver les solutions entières x et y de l'équation

$$x^2(y-1) + y^2(x-1) = 1.$$

Démonstration.

Pour ce faire, faisons un changement de variables. Posons $x = u + 1$, $y = v + 1$, l'équation devient

$$(u+1)^2 v + (v+1)^2 u = 1,$$

qui est équivalente à

$$uv(u+v) + 4uv + (u+v) = 1.$$

Cette équation peut se réécrire sous la forme de :

$$uv(u+v+4) + (u+v+4) = 5$$

ou

$$(u+v+4)(uv+1) = 5.$$

L'un des facteurs doit être égal à 5 ou -5 et l'autre égal à 1 ou -1. Ce qui signifie que la somme $u+v$ et le produit uv doivent satisfaire l'un des quatre systèmes d'équations :

$$\begin{cases} u+v &= 1 \\ uv &= 0 \end{cases}, \quad \begin{cases} u+v &= -9 \\ uv &= -2 \end{cases},$$

$$\begin{cases} u+v &= -3 \\ uv &= 4 \end{cases}, \quad \begin{cases} u+v &= -5 \\ uv &= -6. \end{cases}$$

Seuls le premier et le dernier de ces systèmes ont des solutions intégrales.

Ce sont $(0,1), (1,0), (-6,1), (1,-6)$. D'où le résultat final $(x,y) = (u+1, v+1)$ doit être l'une des paires $(1,2), (-5,2), (2,1), (2,-5)$. □

2.4.2 Résolution utilisant les inégalités

Cette méthode consiste à restreindre les intervalles dans lesquels les variables appartiennent en utilisant les inégalités appropriées. Généralement, ce processus conduit à un nombre infini de possibilités pour toutes les variables ou pour certaines d'entre elles.

Exemple 2.4.5.

Déterminer toutes les paires d'entiers (x, y) telles que :

$$x^3 + y^3 = (x + y)^2. \tag{2.27}$$

Démonstration.

Nous remarquons que toutes les paires de la forme $(k, -k), k \in \mathbb{Z}$, sont solutions de (2.27). Si $x + y \neq 0$, l'équation précédente devient

$$x^2 - xy + y^2 = x + y,$$

qui est équivalente à

$$(x - y)^2 + (x - 1)^2 + (y - 1)^2 = 2.$$

Il s'ensuit que $(x - 1)^2 \leq 1$ et $(y - 1)^2 \leq 1$, restreignant l'intervalle dans lequel les variables x, y appartiennent à $[0, 2]$. Les solutions de l'équation sont donc :

$$(0, 1), (1, 0), (1, 2), (2, 1), (2, 2).$$

□

Nous passons à la méthode paramétrique

2.4.3 Méthode paramétrique

Dans de nombreuses situations, les solutions intégrales d'une équation Diophantienne

$$f(x_1, x_2, \ldots, x_n) = 0$$

peuvent être représentées sous une forme paramétrique comme suit :

$$x_1 = g_1(k_1, ..., k_l), x_2 = g_2(k_1, ..., k_l), ..., x_n = g_n(k_1, ..., k_l),$$

où $g_1, g_2, ..., g_n$ sont des fonctions de l-variables à valeur entière et $k_1, ..., k_l \in \mathbb{Z}$. L'ensemble de solutions de certaines équations Diophantiennes pourrait avoir plusieurs représentations paramétriques. Pour la plupart des équations Diophantiennes, il n'est pas possible de trouver toutes les solutions explicitement. Dans de nombreux cas, la méthode paramétrique

fournit une preuve de l'existence d'une infinité de solutions.

Exemple 2.4.6.

Démontrer qu'il existe une infinité de triplets (x, y, z) d'entiers tels que :

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2.$$

Démonstration.

Si $z = -y$, l'équation devient $x^3 = x^2 + 2y^2$. En prenant $y = mx, m \in \mathbb{Z}$, on obtient $x = 1 + 2m^2$ ainsi que l'infinie famille de solutions :

$$x = 2m^2 + 1, \quad y = m(2m^2 + 1), \quad z = -m(2m^2 + 1), \quad m \in \mathbb{Z}.$$

□

Exemple 2.4.7.

a) *Soit m et n des entiers positifs distincts. Prouver qu'il existe une infinité de triplets (x, y, z) d'entiers positifs tels que $x^2 + y^2 = (m^2 + n^2)^z$, avec*

   i) *z impair ;*

   ii) *z pair.*

b) *Démontrer que l'équation $x^2 + y^2 = 13^z$ a une infinité de solutions entières positives x, y, z.*

Démonstration.

(a) Pour (i), considérons la famille

$$x_k = m(m^2 + n^2)^k, \quad y_k = n(m^2 + n^2)^k, \quad z_k = 2k + 1, \quad k \in \mathbb{N}.$$

Pour (ii), considérons la famille

$$x_k = |m^2 - n^2|(m^2 + n^2)^{k-1}, \quad y_k = 2mn(m^2 + n^2)^{k-1}, \quad z_k = 2k, \quad k \in \mathbb{Z}_+$$

(b) puisque $2^2 + 3^2 = 13$, on peut prendre $m = 2, n = 3$ et obtenir la famille de solutions

$$x'_k = 2 \cdot 13^k, \quad y'_k = 3 \cdot 13^k, \quad z'_k = 2k + 1, \quad k \in \mathbb{Z}_+ ;$$
$$x''_k = 5 \cdot 13^{k-1}, \quad y''_k = 12 \cdot 13^{k-1}, \quad z''_k = 2k, \quad k \in \mathbb{Z}_+.$$

□

Remarque 2.4.2.

1. *Tenant compte de l'identité de Lagrange*

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2,$$

nous pouvons générer une famille infinie de solutions en définissant récursivement les suites $(x_k)_{k\geq 1}, (y_k)_{k\geq 1}$ *comme suit :*

$$\begin{cases} x_{k+1} &= mx_k - ny_k, \\ y_{k+1} &= nx_k + my_k, \end{cases}$$

où $x_1 = m, y_1 = n$. *Il est facile de vérifier que* $(|x_k|, y_k, k), \quad k \in \mathbb{Z}_+$, *sont des solutions à l'équation donnée.*

2. *Une autre façon de générer une famille infinie de solutions est de le faire avec les nombres complexes. Soit k un entier positif. Nous avons* $(m+in)^k = A_k + iB_k, \quad$ *où* $\quad A_k, B_k \in \mathbb{Z}$. *En prenant des modules, on obtient*

$$(m^2+n^2)^k = A_k^2 + B_k^2,$$

et donc $(|A_k|, |B_k|, k)$ *est une solution à l'équation donnée.*

Exemple 2.4.8.

Trouvez tous les triplets (x, y, z) *d'entiers positifs tels que :*

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}.$$

Démonstration.

Cette équation est équivalente à :

$$z = \frac{xy}{x+y}.$$

Soit $d = \text{pgcd}(x, y)$. Alors $x = dm, y = dn$, avec $\text{pgcd}(m, n) = 1$. Il s'ensuit que le $\text{pgcd}(mn, m+n) = 1$. Par conséquent,

$$z = \frac{dmn}{m+n}, \tag{2.28}$$

ce qui implique $(m+n)|d$, c'est-à-dire $d = k(m+n), \quad$ avec $\quad k \in \mathbb{Z}_+$. Les solutions de

l'équation sont données par

$$x = km(m+n), \quad y = kn(m+n), \quad z = kmn, \quad \text{où} \quad k, m, n \in \mathbb{Z}_+.$$

□

Remarque 2.4.3.

(1) Si a, b, c sont des entiers positifs sans facteur commun tels que

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c},$$

alors $a + b$ est un carré. En effet, $k = 1, a = m(m+n), b = n(m+n)$, et donc $a + b = (m+n)^2$.

(2) Si a, b, c sont des entiers positifs qui satisfont

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{c},$$

alors $a^2 + b^2 + c^2$ est un carré. En effet,

$$\begin{aligned} a^2 + b^2 + c^2 =& k^2[m^2(m+n)^2 + n^2(m+n)^2 + m^2n^2] \\ =& k^2[(m+n)^4 - 2mn(m+n)^2 + m^2n^2] \\ =& k^2[(m+n)^2 - mn]^2. \end{aligned}$$

Exemple 2.4.9.

Démontrer que pour chaque entier $n \geq 3$ l'équation

$$x^n + y^n = z^{n-1}$$

a une infinité de solutions entières positives.

Démonstration.

Une famille infinie de solutions est donnée par

$$x_k = k(k^n+1)^{n-2}, \quad y_k = (k^n+1)^{n-2}, \quad z_k = (k^n+1)^{n-1}, \quad k \in \mathbb{Z}_+.$$

□

Exemple 2.4.10.

Soit a, b des entiers positifs. Prouver que l'équation

$$x^2 - 2axy + (a^2 - 4b)y^2 + 4by = z^2$$

a une infinité de solutions entières positives (x_j, y_j, z_j), où $(x_j), (y_j), (z_j)$ sont des suites croissantes.

Démonstration.

Nous utiliserons le résultat auxiliaire suivant :

Lemme 2.4.1.

Si A, B sont des entiers positifs relativement premiers, alors il existe des entiers positifs u, v tels que

$$Au - Bv = 1. \tag{2.29}$$

Démonstration.

Considérons les entiers

$$1 \cdot A, 2 \cdot A, \cdots, (B-1) \cdot A \pmod{B}. \tag{2.30}$$

Tous ces restes sont distincts. En effet, si

$$k_1 A = q_1 B + r \quad \text{et} \quad k_2 A = q_2 B + r$$

pour certains $k_1, k_2 \in 1, 2, ..., B-1$, puis

$$(k_1 - k_2)A = (q_1 - q_2)B \equiv 0 \pmod{B};$$

puisque $\text{pgcd}(A, B) = 1$, il s'ensuit que $|k_1 - k_2| \equiv 0 \pmod{B}$. Tenant compte du fait que $k_1, k_2 \in \{1, 2, ..., B-1\}$, nous avons $|k_1 - k_2| < B$. Ainsi $k_1 - k_2 = 0$.

Il n'est pas difficile de voir que $k \cdot A \equiv 0 \pmod{B}$ pour tout $k \in \{1, 2, ..., B-1\}$. Par conséquent, au moins l'un des nombres entiers (2.30) donne 1 comme reste de la division par B, c'est-à-dire qu'il existe $u \in \{1, 2, ..., B-1\}$ et $v \in \mathbb{Z}_+$ tels que $A \cdot u = B \cdot v + 1$. □

□

Nous allons présenter la méthode arithmétique modulaire.

2.4.4 Méthode arithmétique modulaire

Dans de nombreuses situations, de simples considérations arithmétiques modulaires sont utilisées pour prouver que certaines équations Diophantiennes n'admettent pas de solution.

Exemple 2.4.11.

Démontrez que l'équation

$$(x+1)^2 + (x+2)^2 + ... + (x+2001)^2 = y^2 \tag{2.31}$$

n'admet pas de solution.

Démonstration.

Soit $x = z - 1001$. L'équation précédente devient

$$(z-1000)^2 + ... + (z-1)^2 + z^2 + (z+1)^2 + ... + (z+1000)^2 = y^2,$$

ou

$$2001z^2 + 2(1^2 + 2^2 + ... + 1000^2) = y^2.$$

Il s'ensuit que

$$2001z^2 + 2\frac{1000 \times 1001 \times 2001}{6} = y^2,$$

ou équivalent,

$$2001z^2 + 1000 \times 1001 \times 667 = y^2. \tag{2.32}$$

Le terme du côté gauche est congru à $2 \pmod 3$, donc il n'est pas un carré parfait. □

2.4.5 Méthode d'induction mathématique

L'induction mathématique est une méthode puissante et élégante pour prouver un énoncé dépendant d'entiers positifs. Soit $(P(n))_{n\geq 0}$ une suite de propositions. La méthode de l'induction mathématique nous aide à prouver que $P(n)$ est vrai pour tous $n \geq n_0$, où n_0 est un entier positif donné.

Énoncé : Induction mathématique (forme faible) : Supposons que :

- $P(n_0)$ est vraie ;
- Pour tout $k \geq n_0$, $P(k)$ est vraie implique $P(k+1)$ est vraie.

Alors $P(n)$ est vraie pour tout $n \geq n_0$.

Énoncé : Induction mathématique (avec étape s) : Soit s un entier positif fixe. Supposons que :

- $P(n_0), P(n_0+1), ..., P(n_0+s-1)$ sont vraies ;
- Pour tout $k \geq n_0$, $P(k)$ est vraie implique que $P(k+s)$ est vraie.

Alors $P(n)$ est vraie pour tout $n \geq n_0$.

Énoncé : Induction mathématique (forme forte) : Supposons que

- $P(n_0)$ est vraie ;
- Pour tout $k \geq n_0$, $P(m)$ est vraie pour tout m avec $n_0 \leq m \leq k$ implique $P(k+1)$ est vraie.

Alors $P(n)$ est vraie pour tout $n \geq n_0$. Cette méthode est largement utilisée dans divers domaines des mathématiques, y compris la théorie des nombres. Les exemples suivants sont destinés à montrer comment l'induction mathématique fonctionne dans l'étude des équations Diophantiennes.

Exemple 2.4.12.
Démontrer que pour tous les entiers $n \geq 3$, il existe des entiers positifs x et y qui sont impairs tels que

$$7x^2 + y^2 = 2^n. \tag{2.33}$$

Démonstration.
Nous prouverons qu'il existe des entiers positifs x_n, y_n qui sont impairs tels que $7x_n^2 + y_n^2 = 2^n, n \geq 3$. Pour $n = 3$, nous avons $x^3 = y^3 = 1$. Supposons maintenant que pour un entier $n \geq 3$ donné, nous avons des entiers impairs x_n, y_n satisfaisant $7x_n^2 + y_n^2 = 2^n$. Nous allons montrer qu'il existe des entiers positifs impairs (x_{n+1}, y_{n+1}) tels que $7x_{n+1}^2 + y_{n+1}^2 = 2^{n+1}$. En effet,

$$7\left(\frac{x_n \pm y_n}{2}\right) + \left(\frac{7x_n \pm y_n}{2}\right) = 2(7x_n^2 + y_n^2) = 2^{n+1}.$$

Précisément l'un des nombres $\frac{x_n+y_n}{2}$ et $\frac{|x_n-y_n|}{2}$ est impair. Si, par exemple, $\frac{x_n+y_n}{2}$ est impair, alors

$$\frac{7x_n - y_n}{2} = 3x_n + \frac{x_n - y_n}{2}$$

est impair (comme somme d'un nombre pair et impair) ; dans ce cas, nous pourrions choisir

$$x_{n+1} = \frac{x_n + y_n}{2} \quad \text{et} \quad y_{n+1} = \frac{7x_n - y_n}{2}.$$

Si $\frac{x_n - y_n}{2}$ est impair, alors

$$\frac{7x_n + y_n}{2} = 3x_n + \frac{x_n + y_n}{2},$$

donc

$$x_{n+1} = \frac{|\, x_n - y_n \,|}{2} \quad \text{et} \quad y_{n+1} = \frac{7x_n + y_n}{2}.$$

□

Nous allons présenter dans la section suivante la méthode de descente infinie de Fermat.

2.4.6 Méthode de descente infinie de Fermat

Pierre de Fermat $(1601 - 1665)$ est célèbre pour ses contributions en mathématiques même s'il n'était considéré que comme un mathématicien amateur. Il a obtenu son diplôme en droit civil à l'Université d'Orléans avant 1631 et servi comme avocat puis conseiller à Toulouse.

Fermat a eu un impact énorme sur le monde des mathématiques à travers ses découvertes et ses méthodes. Il fut l'un des premiers mathématiciens à utiliser une méthode appelée «descente infinie». Soit P une propriété concernant les entiers positifs et soit $(P(n))_{n\geq 1}$ une suite de propositions,

$$P(n) : \text{«}n \text{ satisfait la propriété } P.\text{»}$$

La méthode suivante est utile pour prouver que la proposition $P(n)$ est fausse pour tout n assez grand . Soit k un entier positif. Supposons que :

- $P(k)$ n'est pas vraie ;
- chaque fois que $P(m)$ est vraie pour un entier positif $m > k$, alors il existe un petit j, $m > j \geq k$, pour lequel $P(j)$ est vraie.

Alors $P(n)$ est fausse pour tout $n \geq k$.

La méthode décrite ci-dessus est souvent appelée la méthode de descente finie. La méthode de descente infinie de Fermat peut être reformulée comme suit : Soit k un entier positif. Supposons que :

- chaque fois que $P(m)$ est vraie pour un entier $m > k$, il existe un petit $j, m > j > k$, pour lequel $P(j)$ est vraie.

Alors $P(n)$ est fausse pour tout $n > k$. Autrement dit, s'il y avait un n pour lequel $P(n)$ était vraie, on pourrait construire une suite $n > n_1 > n_2 > ...$ qui serait tous supérieurs à k, mais pour les entiers positifs, aucune suite décroissante infinie n'existe.

Deux cas particuliers de la descente infinie de Fermat sont particulièrement utiles dans l'étude des équations Diophantiennes.

- **Variante 1 :** Il n'y a pas de suite d'entiers positifs $n_1 > n_2 > \cdots$.

  Dans certaines situations, il est commode de remplacer **Variante 1** par la forme équivalente suivante : Si n_0 est le plus petit entier positif n pour lequel $P(n)$ est vraie alors $P(n)$ est fausse pour tout $n < n_0$.

- **Variante 2 :** Si la suite d'entiers positifs $(n_i)_{i\geq 1}$ vérifie les inégalités $n_1 \geq n_2 \geq \cdots$, alors il existe i_0 tel que $n_{i_0} = n_{i_0+1} = \cdots$.

Exemple 2.4.13.
Trouver les solutions entières de l'équation

$$x^3 + 2y^3 = 4z^3. \tag{2.34}$$

Démonstration.
Notez que $(0,0,0)$ est solution de l'équation (2.34). Nous prouverons qu'il n'y a pas d'autres solutions. Supposons que (x_1, y_1, z_1) est une solution non triviale. $\sqrt[3]{2}$ et $\sqrt[3]{4}$ étant tous irrationnels, il n'est pas difficile de voir que $x_1 > 0, y_1 > 0, z_1 > 0$. De $x_1^3 + 2y_1^3 = 4z_1^3$, il s'ensuit que $2|x_1$, donc $x_1 = 2x_2, x_2 \in \mathbb{N}$. Alors $4x_2^3 + y_1^3 = 2z_1^3$, et donc $y_1 = 2y_2, y_2 \in \mathbb{N}$. De même, $z_1 = 2z_2, z_2 \in \mathbb{N}$. On obtient la «nouvelle» solution (x_2, y_2, z_2) avec $x_1 > x_2, y_1 > y_2, z_1 > z_2$. Poursuivant cette analyse, nous construisons une suite de solutions intégrales positives $(x_n, y_n, z_n)_{n\geq 1}$ telles que $x_1 > x_2 > x_3 > ....$ Mais cela contredit **la variante 1**. □

Cette méthode a permis à Legendre de résoudre le grand théorème de Fermat dans les cas $n = 4$ et $n = 5$.

A présent, les notions de bases en théorie des nombres, les suites récurrentes linéaires et les équation Diophantiennes ayant été abordées, dans la suite, il sera question de discuter d'une notion très importante : les formes linéaires de logarithmes. Cette méthode est une double

application de la méthode de Baker et de quelques calculs avec des fractions continues pour réduire la plage de recherche de force brute sur les variables. Face à certaines équations, les méthodes classiques deviennent inefficaces et c'est grâce à l'approche transcendantale introduite par le mathématicien Britannique A. Baker qu'on arrive à bout de ces équations.

Chapitre 3

FORMES LINÉAIRES DE LOGARITHMES

3.1 Formes linéaires de Logarithmes

Nous allons rappeler les résultats de la théorie de la transcendance, puis travailler sur les bornes inférieures des formes linéaires de logarithmes des nombres algébriques, qui sont d'une grande importance pour résoudre efficacement les équations Diophantiennes exponentielles. Pour plus de détails et preuves, nous renvoyons le lecteur aux livres de Baker [22], et de Shorey et Tijdeman [23].

Nous savons qu'un nombre algébrique est un élément de $\mathbb{C}$ qui est racine de polynôme à coefficients dans $\mathbb{Q}$ (ou à coefficients entiers). Une question naturelle nous vient à l'esprit : tout nombre complexe est-il algébrique ? Tout nombre complexe qui n'est pas algébrique est un nombre transcendant.

Liouville en 1844, a prouvé le théorème suivant :

Théorème 3.1.1 (Liouville)**.**
Soit α un nombre algébrique de degré $d > 1$. Il existe un nombre positif C effectivement calculable en terme de α tel que

$$\left|\alpha - \frac{p}{q}\right| > \frac{C(\alpha)}{q^d}$$

pour $p, q \in \mathbb{Z}$, $q > 0$.

Ce théorème a permis à Liouville de construire les premiers nombres transcendants, par exemple

$$\sum_{n=0}^{\infty} b^{n!}$$

avec $0 < b < 1$.

Nous obtenons ainsi la réponse à notre question. Il existe en effet, des nombres transcendants.

En 1874, Cantor a prouvé que les nombres transcendants sont denses dans $\mathbb{R}$ en partant du fait que les nombres algébriques sont dénombrables. Cependant, il n'est pas facile de les trouver, ni de prouver qu'un nombre complexe est transcendant.

De même, Hermite a prouvé la transcendance de e en 1874 et Lindemann celle de π en 1882.

Aussi, En 1900, Hilbert propose comme 7ème problème lors du congrès international de mathématiques ce qui suit : si α est un nombre algébrique et $\alpha \neq 0, 1$ et β un nombre algébrique irrationnel, alors α^β est transcendant ; qui a été aussi prouvé par Gelfond et Schneider indépendamment en 1934.

Leur résultat se présente sous forme de théorème comme suit :

Théorème 3.1.2 (Gelfond–Schneider)**.**
Soit α, β des nombres algébriques dans $\mathbb{C}$, avec $\alpha \neq 0; 1$ et $\beta \notin \mathbb{Q}$. Alors α^β est transcendant.

Dans le Théorème 3.1.2, $\alpha^\beta := e^{\beta \log \alpha}$, où $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ et $\log \alpha = \log |\alpha| + i\text{arg}\alpha$ car $\alpha = |\alpha| e^{i arg \alpha}$. L'argument de α est déterminé seulement comme multiple de 2π. Donc, $\log \alpha$ ainsi que α^β sont des multi-valeurs. Le théorème 3.1.2 est valable pour toute valeur de $\text{arg}\alpha$.

Ci-dessous présentés, quelques corollaires immédiats.

Corollaire 3.1.1.
Soit α un nombre algébrique complexe avec $i\alpha \in \mathbb{Q}$. Alors $e^{\pi\alpha}$ est transcendant.

Corollaire 3.1.2.
Soient α, β des nombres algébriques de $\mathbb{C}$, avec $\alpha; \beta \neq 0; 1$ tels que $\log \alpha$ et $\log \beta$ soient linéairement indépendants sur $\mathbb{Q}$. Alors, pour tous nombres algébriques non nul γ et η de $\mathbb{C}$ on a :

$$\gamma \log \alpha + \eta \log \eta \neq 0.$$

Énonçons à présent un résultat de Baker publié 1966, qui est une généralisation du Corollaire 3.1.2 aux formes linéaires des nombres algébriques arbitraires de logarithmes.

Théorème 3.1.3 (A. Baker)**.**
Soient $\alpha_1, ..., \alpha_n$ des nombres algébriques dans $\mathbb{C}$ qui sont différents de $0, 1$ et tels que $\log \alpha_1, ..., \log \alpha_n$

sont linéairement indépendants sur $\mathbb{Q}$. *Alors, pour tout n-uplet* $(\beta_0, \beta_1, ..., \beta_n)$ *de nombres algébriques dans* $\mathbb{C}$ *différents de* $(0, 0, ..., 0)$, *on a :*

$$\beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n \neq 0.$$

Pour les applications aux équations Diophantiennes, il est important que la forme linéaire ci-dessus soit différente de zéro, mais aussi que nous ayons une borne inférieure suffisamment forte pour la valeur absolue de cette forme linéaire. Ci-dessous, nous indiquons un résultat de Baker(1975), qui est un cas particulier où $\beta_0 = 0$ et $\beta_1, \beta_2, ..., \beta_n$ sont des entiers rationnels. C'est le seul cas qui a une application dans la résolution des équations Diophantiennes. Rappelons que la méthode de Baker ne s'applique que sur les équations Diophantiennes exponentielles. On utilise souvent les méthodes arithmétiques élémentaires pour résoudre les autres types d'équations Diophantiennes comme nous l'avons vu dans la section 2.4 du Chapitre 2.

Théorème 3.1.4 (A. Baker)**.**
Soient $\alpha_1, ..., \alpha_n$ *des nombres algébriques de* $\mathbb{C}$ *différents de* $0, 1$. *De plus, soient* $b_1, ..., b_n$ *des nombres rationnels tels que*

$$b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n \neq 0.$$

Alors,

$$|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| \geqslant (eB)^{-C}$$

où $B := \max\{|b_1|, ..., |b_n|\}$ *et C est une constante effectivement calculable dépendante seulement de n et* $\alpha_1, ..., \alpha_n$.

Que signifie constante effectivement calculable ? C est une constante effectivement calculable signifie qu'en passant par la preuve du Théorème 3.1.4, on peut calculer une valeur explicite de C. Il est également possible de se débarrasser du logarithme.

Le théorème 3.1.4 conduit aux corollaires suivants :

Corollaire 3.1.3.
Soient $\alpha_1, \ldots, \alpha_n$ *des nombres algébriques de* $\mathbb{C}$ *différents de* $0, 1$ *et soit* $b_1, \ldots, b_n$ *des entiers rationnels tels que :*

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1.$$

Alors,

$$\left|\alpha_1^{b_1}\cdots\alpha_n^{b_n}-1\right|\geq (eB)^{-C'},$$

où $B:=\max\{|b_1|,\ldots,|b_n|\}$ *et* C' *est une constante effectivement calculable dépendant uniquement de* n *et de* $\alpha_1,\ldots,\alpha_n$.

Pour être complet, nous donnons le résultat de Matveev, qui est une version complètement explicite de la version du corollaire 3.1.3 lorsque $\alpha_1,\ldots,\alpha_n$ sont des nombres rationnels. Avant de donner le théorème de Matveev, définissons d'abord une notion importante : *la hauteur d'un nombre algébrique*. Pour ce faire, nous définissons d'abord la notion mesure de Malher.

3.2 Mesure de Malher

3.2.1 Mesure de Malher d'un polynôme

Étudier la complexité d'un nombre algébrique α peut se faire en donnant une mesure de complexité de son polynôme minimal sur $\mathbb{Z}$ (c'est-à-dire le seul polynôme irréductible, à coefficients entiers rationnels, de coefficient dominant positif, s'annulant en α). Pour mesurer la complexité d'un polynôme

$$f(X)=a_dX^d+a_{d-1}X^{d-1}+\cdots+a_0$$

à coefficients dans $\mathbb{Z}$, une approche standard consiste à utiliser les différentes normes définies sur $\mathbb{C}[X]$:

$$\begin{aligned}\|f\|_1&=|a_0|+\cdots+|a_d|,\\ \|f\|_2&=\sqrt{|a_0|^2+\cdots+|a_d|^2},\\ \|f\|_\infty&=\max(|a_0|,\ldots,|a_d|),\\ |f|_1&=\max|f(z)|\quad\text{pour}\quad|z|=1,\end{aligned}$$

que l'on nomme respectivement longueur, norme quadratique (ou euclidienne), hauteur (ou hauteur naïve), et norme de la convergence uniforme sur la boule unité. Les relations parmi ces normes sont résumées dans la proposition suivante :

Proposition 3.2.1.

Pour tout polynôme $f \in \mathbb{C}[X]$ de degré au plus d, nous avons

$$\|f\|_\infty \leq \|f\|_2 \leq |f|_1 \leq \|f\|_1 \leq (d+1)\,\|f\|_\infty .$$

Toutes ces inégalités sont évidentes, à l'exception peut-être de l'inégalité $\|f\|_2 \leq |f|_1$. Cette dernière découle cependant du lemme suivant, que l'on démontre facilement à l'aide de la formule de *Parseval* .

L'égalité de *Parseval* dite parfois théorie de *Parseval* ou relation de *Parseval* est une formule fondamentale de la théorie des séries de Fourier. Cette formule peut être interprétée comme une généralisation du théorème de Pythagore pour les espaces de Hilbert. Sa formule pour les séries de Fourier s'énonce comme suit : Soit f une fonction $T-$périodique et de carré intégrable sur une période. On définit ses coefficients de Fourier.

$$c_n = \frac{1}{T}\int_{-T/2}^{T/2} f(t)e^{-in\frac{2\pi}{T}t}dt.$$

L'égalité de *Parseval* affirme la convergence de la série suivante et énonce l'identité :

$$\sum_{n=-\infty}^{+\infty} |c_n|^2 = \frac{1}{T}\int_{-T/2}^{T/2} |f(t)|^2 dt = \|f\|^2 .$$

Si la fonction est à valeur réelle, on peut adopter les conventions suivantes :

- $a_0 = \dfrac{1}{T}\displaystyle\int_{-T/2}^{T/2} f(t)dt = c_0$;
- $a_n = \dfrac{2}{T}\displaystyle\int_{-T/2}^{T/2} f(t)\cos\frac{2\pi nt}{T}dt$;
- $b_n = \dfrac{2}{T}\displaystyle\int_{-T/2}^{T/2} f(t)\sin\frac{2\pi nt}{T}dt.$

L'égalité de *Parseval* devient $\|f\|^2 = a_0^2 + \dfrac{1}{2}\displaystyle\sum_{n=1}^{+\infty}\left(a_n^2 + b_n^2\right).$

Remarque 3.2.1.

Certains auteurs préfèrent une convention pour laquelle l'expression de a_0 est aussi une expression en $2/T$:

$$a_0 = \frac{2}{T}\int_{-T/2}^{T/2} f(t)dt.$$

La formule devient

$$\|f\|^2 = \frac{1}{4}a_0^2 + \frac{1}{2}\sum_{n=1}^{+\infty}\left(a_n^2 + b_n^2\right).$$

Lemme 3.2.1.

Pour tout polynôme $f \in \mathbb{C}[X]$, on a :

$$\|f\|_2^2 = \frac{1}{2\pi}\int_0^{2\pi} |f(e^{it})|^2 dt,$$

Il est clair que chacune des normes introduites mesure dans un sens, la complexité d'un polynôme à coefficients entiers f (par exemple, la longueur donne une idée du nombre de chiffres nécessaires à l'écriture de f). Cependant il serait préférable de disposer d'une mesure canonique de la complexité d'un polynôme. Nous allons définir, pour cela, la mesure de Mahler qui répondra à cette exigence en ayant plus des propriétés arithmétiques suffisamment agréables.

Définition 3.2.1.

Soit $f \in \mathbb{C}[X]$ un polynôme non nul et notons $\mathrm{M}(f)$ le nombre réel défini par :

$$\mathrm{M}(f) = |a| \prod_{j=1}^{d} \max\{1, \alpha_j\}.$$

On note aussi $\mathrm{M}(0) = 1$.

La mesure de Mahler d'un polynôme f est le produit du module de son coefficient dominant et des modules de ses racines en dehors du disque unité (avec leur multiplicité).

Définition 3.2.2.

Soit α un nombre complexe algébrique. On appelle mesure de Mahler de α, et l'on note $M(\alpha)$ la mesure de Mahler du polynôme minimal sur $\mathbb{Z}$ de α.

On déduit de la définition de la mesure de Mahler les propriétés suivantes valables pour tout $f, g \in \mathbb{C}[X]$:

1. $\mathrm{M}(fg) = \mathrm{M}(f)\mathrm{M}(g)$.
2. $\mathrm{M}(f)$ est minorée par la valeur absolue du coefficient dominant de f.
3. $\mathrm{M}(f(X^n)) = \mathrm{M}(f)$, pour tout entier $n \geq 1$.
4. $\mathrm{M}(f^*) = \mathrm{M}(f)$, où f^* désigne le polynôme réciproque de f (défini par

$$f^*(X) = X^{\deg(f)} f(X^{-1})).$$

La mesure de Mahler avait déjà été introduite par de nombreux auteurs (notamment par D. H. Lehmer, [56]), mais elle est connue sous ce nom depuis une série d'articles de K. Mahler relatifs à cette quantité parus dans les années 1960. Le théorème suivant qui donne une expression analytique de la mesure de Mahler d'un polynôme, est l'un des résultats élégants montrés par K. Mahler :

Théorème 3.2.1.
Soit $f \in \mathbb{C}[X]$, nous avons :

$$\mathrm{M}(f) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi} \log(|f(e^{it})|)dt\right).$$

Démonstration.
La preuve peut être déduite facilement de la formule de Jensen d'analyse complexe. Pour plus de détails, se référer à [21]. □

3.2.2 Majoration de la mesure de Malher

Nous pouvons comparer la mesure de Mahler avec les normes introduites au début du paragraphe précédent. Commençons par majorer cette mesure en fonction des normes $\|f\|_1, \|f\|_2, \|f\|_\infty, |f|_1$. Au vu de la proposition 3.2.1, il suffit de majorer $M(f)$ en fonction de la norme euclidienne ; le résultat plus précis que l'on connaît est le suivant :

Théorème 3.2.2 (Landeau)**.**
Pour tout polynôme $f \in \mathbb{C}[X]$, nous avons

$$\mathrm{M}(f) \leq \|f\|_2.$$

Démonstration.
Se référer au théorème 1.2.1 de [21] pour des détails sur la preuve. □

3.2.3 Minoration de la mesure de Malher

Nous allons maintenant minorer la mesure de Mahler en fonction des normes introduites. Pour ce faire, nous avons besoin du lemme suivant :

Lemme 3.2.2.
Soit $f(X) = a_d X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{C}[X]$ *un polynôme de degré* d. *Pour* $j = 1, \ldots, d$, *nous avons*

$$|a_j| \leq \binom{d}{k} \mathrm{M}(f).$$

Démonstration. Se référer au Lemme 1.3.1 de [21] pour plus de détails. □

En utilisant ce lemme, on en déduit le résultat suivant.

Théorème 3.2.3 (F. Amoroso et D. Vergnaud)**.**
Pour tout polynôme $f \in \mathbb{C}[X]$ *de degré* $\leq d$, *nous avons*

$$\|f\|_2 \leq \binom{2d}{d}^{1/2} \mathrm{M}(f), \tag{3.1}$$

$$|f|_1 \leq 2^d \mathrm{M}(f), \tag{3.2}$$

$$\|f\|_1 \leq 2^d \mathrm{M}(f), \tag{3.3}$$

$$\|f\|_\infty \leq \binom{d}{\lfloor d/2 \rfloor} \mathrm{M}(f), \tag{3.4}$$

où $\lfloor x \rfloor$ *désigne la partie entière inférieure de* x.

Démonstration.
Pour montrer (3.1), (3.3) et (3.4), il suffit d'appliquer le Lemme 3.2.2. Pour plus de détails, confère [21]. □

Abordons à présent les notions de hauteur naïve et de hauteur logarithmique absolue.

3.2.4 Hauteur algébrique

Dans cette section, nous allons introduire la notion de hauteur algébrique qui est très utile comme nous le verrons dans la suite. Nous commençons par définir la hauteur naïve et par suite déduire d'elle, la hauteur logarithmique absolue.

Définition 3.2.3 (Hauteur naïve)**.**
Pour tout nombre algébrique γ, *on définit la hauteur de* γ *par :*

$$H(\gamma) = \max(|a_d|, \ldots, |a_0|),$$

où $f(x) = a_d x^d + \cdots + a_1 x + a_0$ est un polynôme minimal de γ sur $\mathbb{Z}$. $H(\gamma)$ est appelée hauteur naïve de γ.

Exemple 3.2.1.

Soit α un nombre algébrique :

- *Si $\gamma \in \mathbb{Z}$, $H(\gamma) = |\gamma|$.*
- *Si $\gamma \in \mathbb{Q}$ $\left(i.e.\ \gamma = \dfrac{b}{a}\ avec\ pgcd(a,b) = 1\right)$, $H(\gamma) = \max\{|a|, |b|\}$,*

Pour tout nombre algébrique γ, on a l'identité suivante :

$$H(\gamma) = |a_d| \prod_{i=1}^{d} \max\{1, |\gamma_i|\}, \tag{3.5}$$

où γ_i représentent les racines du polynôme minimal et $f(x) = a_d \prod_{i=1}^{d} (x - \gamma^{(i)})$ est le polynôme minimal de γ. On définit dans la sous-section suivante, une autre hauteur déduite de la précédente appelée hauteur logarithmique absolue. Elle est la plus utilisée.

Définition 3.2.4 (Hauteur logarithmique absolue)**.**

Pour un nombre algébrique non nul de degré d sur $\mathbb{Q}$ où le polynôme minimal sur $\mathbb{Z}$ est $f(x) = a_d \prod_{i=1}^{d} (x - \gamma^{(i)})$, on dénote par :

$$h(\gamma) = \frac{1}{d}\left(\log |a_d| + \sum_{i=1}^{d} \log \max\{1, |\gamma^i|\}\right) = \frac{1}{d} \log \mathrm{M}(\gamma), \tag{3.6}$$

la hauteur logarithmique absolue usuel de γ.

Les propriétés de la hauteur logarithmique absolue sont les suivantes :

Proposition 3.2.2 (Y. F. Bilu, Y. Bugeaud et M. Mignotte)**.**

1. *Soient γ, δ deux nombres algébriques non nuls. On a*
   - $h(\gamma\delta) \leq h(\gamma) + h(\delta)$,
   - $h(\gamma + \delta) \leq h(\gamma) + h(\delta) + \log 2$.
2. *Pour tout nombre algébrique γ et $n \in \mathbb{Z}$ (avec $\gamma \neq 0$ et si $n < 0$) on a :* $h(\gamma^n) = |n| h(\gamma)$.

Plus généralement, pour $\gamma_1, \gamma_2, \cdots, \gamma_n$, n nombres algébriques, on a :

- $h(\gamma_1\gamma_2\cdots\gamma_n) \leq h(\gamma_1) + h(\gamma_2) + \cdots + h(\gamma_n)$
- $h(\gamma_1 + \gamma_2 + \cdots + \gamma_n) \leq h(\gamma_1) + h(\gamma_2) + \cdots + h(\gamma_n) + \log n$.

Exemple 3.2.2.

Soit γ un nombre algébrique

1. *Si γ est la racine de $x^2 - 2x - 1$, alors $h(\gamma) = \frac{1}{2}(\log\max\{1, |\alpha|\} + \log\max\{1, |\beta|\})$, $\alpha = 1 + \sqrt{2}$ et $\beta = 1 - \sqrt{2}$, alors $h(\gamma) = \frac{1}{2}\log\alpha$.*
2. *Soit à déterminer $h(\gamma)$ avec $\gamma = \dfrac{\alpha^n - 1}{2\sqrt{2}}$ où $\alpha = 1 + \sqrt{2}$. D'après les propositions (9.1) et (9.2), on sait que $2\sqrt{2}P_n = \alpha^n - \beta^n$ et $Q_n = \alpha^n + \beta^n$.*

Alors,

$$\begin{aligned}
4\sqrt{2}\gamma + 2 &= 2\sqrt{2}P_n + Q_n \\
4\sqrt{2}\gamma - 2\sqrt{2}P_n &= Q_n - 2 \\
8(4\gamma^2 - 4P_n\gamma + P_n^2) &= Q_n^2 - 4Q_n + 4 \\
8(4\gamma^2 - 4P_n\gamma) &= Q_n^2 - 8P_n^2 - 4Q_n + 4 \\
8(4\gamma^2 - 4P_n\gamma) &= 4(-1)^n - 4Q_n + 4.
\end{aligned}$$

On obtient le polynôme minimal de γ divise $8x^2 - 8P_nx - ((-1)^n + 1 - Q_n)$. Ce qui implique $a(x - \gamma)(x - 1 + \gamma)$ avec $a \in \{1, 2, 4, 8\}$.

$$h(\gamma) = \frac{1}{a}\left(\log a + \log\max\{1, |\gamma|\} + \log\max\{1, |1 - \gamma|\}\right).$$

Énonçons à présent les théorèmes de Stewart, Baker et Wüstholz, avant celui de Matveev.

Théorème 3.2.4 (1993, Baker et Wustholz)**.**

Si $\Lambda \neq 0$, alors

$$|\Lambda| > \exp\left(-(16nd)^{2n+4}.\log A_1 ... \log A_n.\log B\right) \tag{3.7}$$

avec $A_i = \max\{H(\alpha_i), e\}$, pour $i = 1, \cdots, n$; $B = \max\{|b_1|, \cdots, |b_n|, e\}$ et $d = [\mathbb{Q}(\alpha_1, \cdots, \alpha_n) : \mathbb{Q}]$.

Théorème 3.2.5 (A. Baker et G. Wüstholz)**.**

Soit K le corps de nombres algébriques généré par $\alpha_1, \cdots, \alpha_n$ de degré d sur $\mathbb{Q}$. Soient $\alpha_1, \cdots, \alpha_n \in K^*$ et $b_1, \cdots, b_n \in \mathbb{Z}^*$.

Supposons que $B^* = \max\{|b_1|, \cdots, |b_n|\}$ et $w = A_1A_2...A_n$ avec $|\Lambda| \geq \dfrac{1}{d}\left(\max\{h(\alpha_j), |\log(\alpha_j)|, 1\}\right)$ $(1 \leq j \leq n)$.

Supposons aussi que $\Gamma \neq 0$, alors ;

$$\log(|\Gamma|) > -18(n+1)!n^{n+1}(32d)^{n+2}w\log(2nd)\log(B^*).$$

Énonçons à présent le résultat de E. Matveev [35] qui est le plus utilisé pour résoudre certaines équations Diophantiennes.

Théorème 3.2.6 (E. M. Matveev)**.**
Soit K un corps algébrique des nombres de degré d sur $\mathbb{Q}$. Si $K \subset \mathbb{R}$, on pose $\xi = 1$ sinon $\xi = 2$. Soient $\alpha_1, \ldots, \alpha_n \in \mathbb{K}^*$ et $b_1, \ldots, b_n \in \mathbb{Z}^*$. Supposons

$$B^* = \max\{|b_1|, \ldots, |b_n|\},\ w = A_1A_2 \ldots A_n,\ A_j \geq \max\{dh(\alpha_j), |\log(\alpha_j), 0.16|\}$$

avec $(1 \leq j \leq n)$ et

$$\Gamma = b_1\log(\alpha_1) + \cdots + b_n\log(\alpha_n).$$

Si $\Gamma \neq 0$, alors

$$\log(|\Gamma|) > -C_1(n)d^2w\log(ed)\log(eB^*)$$

avec

$$C_1(n) > \min\{\frac{1}{\xi}(0.5en)^{\xi}30^{n+3}n^{3.5}, 2^{6n+20}\}.$$

Plus simplement, Y. Bugeaud, M. Mignotte et S. Siksek ont établi le résultat suivant.

Théorème 3.2.7 (Y. Bugeaud, M. Mignotte et S. Siksek)**.**
Soit $n \geq 1$ un entier. Soit K le corps des nombres algébriques de degré d. Soient $\alpha_1, ..., \alpha_n$ des éléments non nuls de K et soient $b_1, b_2, ..., b_n$ des entiers,

$$B = \max\{|b_1|, ..., |b_n|\},$$

et

$$\Lambda = \alpha_1^{b_1}...\alpha_n^{b_n} - 1.$$

Soient $A_1, ..., A_n$ des nombres réels tels que

$$A_j \geq \max\{dh(\alpha_j), |\log(\alpha_j), 0.16|\},\ 1 \leq j \leq n.$$

Assumons que $\Lambda \neq 0$, on a ainsi :

$$\log|\Lambda| > -3 \times 30^{n+4} \times (n+1)^{5.5} \times d^2 \times A_1...A_n(1+\log d)(1+\log nB).$$

Si K est réel, alors

$$\log|\Lambda| > -1.4 \times 30^{n+3} \times (n)^{4.5} \times d^2 \times A_1 ... A_n (1+\log d)(1+\log B).$$

On remarque que pour certaines valeurs de n, la borne inférieure du logarithme proposé par E.M. Matveev est meilleure (légèrement) que celle de Baker et Wüstholz.

Lorsque $n = 2$ et α_1, α_2 multiplicativement indépendants, nous avons ces quelques résultats obtenus par Laurent, Mignotte, Nesterenko ([16], Corollaire 2, pp. 288).

Soit dans ce cas B_1, B_2 des nombres réels plus grands que 1 tels que :

$$\log B_i \geq \max\left\{h(\alpha_i), \frac{|\log \alpha_i|}{d}, \frac{1}{d}\right\} \quad \text{pour} \quad i = 1, 2,$$

et posons

$$b' := \frac{|b_1|}{d \log B_2} + \frac{|b_2|}{d \log B_1}.$$

Posons

$$\Gamma := b_1 \log \alpha_1 + b_2 \log \alpha_2.$$

Remarquons que $\Gamma \neq 0$ car α_1 et α_2 sont multiplicativement indépendants.

Théorème 3.2.8 (Laurent, Mignotte, Nesterenko)**.**
Avec les notations précédentes, soient α_1, α_2 des nombres positifs multiplicativement indépendants, alors :

$$\log|\Gamma| > -24.34 d^4 \left(\max\left\{\log b' + 0.14, \frac{21}{d}, \frac{1}{2}\right\}\right)^2 \log B_1 \log B_2.$$

Notons qu'avec $\Gamma := b_1 \log \alpha_1 + b_2 \log \alpha_2$, on a $e^\Gamma - 1 = \Lambda$, où $\Lambda := \alpha_1^{b_1} \cdots \alpha_n^{b_n}$ dans le cas où $n = 2$.

3.2.5 Méthode de réduction

Lors des calculs, nous obtenons des bornes supérieures sur nos variables qui sont trop grandes, nous devons donc les réduire. Pour ce faire, nous utilisons certains résultats de la théorie des fractions continues.

Concernant le traitement des formes linéaires homogènes en deux variables entières, nous utilisons la méthode bien connue du résultat classique dans la théorie de l'approximation

Diophantienne.

Lemme 3.2.3 (Legendre)**.**
Soit τ un nombre irrationnel, $\frac{p_0}{q_0}, \frac{p_1}{q_1}, \frac{p_2}{q_2}, \ldots$ tous les convergents de la fraction continue de τ, et M un entier positif. Soit N un entier positif tel que $q_N > M$. Alors en posant $a(M) := \{a_i : i = 0, 1, 2, \ldots, N\}$, l'inégalité

$$\left|\tau - \frac{r}{s}\right| > \frac{1}{(a(M)+2)s^2},$$

est valable pour toutes les paires (r, s) d'entiers positifs avec $0 < s < M$.

Pour une forme linéaire non homogène à deux variables entières, on utilise une légère variation d'un résultat dû à Dujella et Pethő ([36], Lemme 5a). La preuve est presque identique à celle du résultat correspondant dans [36]. Pour un nombre réel X, on écrit $\|X\| := \min\{|\ X - n\ |: n \in \mathbb{Z}\}$ pour la distance de X au plus proche entier.

Lemme 3.2.4 (Dujella, Pethő)**.**
Soit M un entier positif, $\frac{p}{q}$ un convergent de la fraction continue du nombre irrationnel τ tel que $q > 6M$, et A, B, μ des nombres algébriques tels que $A > 0$ et $B > 1$. En outre, $\varepsilon := \|\mu q\| - M\|\tau q\|$. Si $\varepsilon > 0$, alors l'inégalité suivante :

$$0 < |u\tau - v + \mu| < AB^{-w},$$

n'admet pas de solution entière u, v et w avec

$$u \leq M \quad et \quad w \geq \frac{\log(Aq/\varepsilon)}{\log B}.$$

À diverses occasions, nous devons trouver une borne inférieure pour les formes linéaires de logarithmes avec des coefficients entiers bornés en trois et quatre variables. Dans ce cas, nous utilisons l'algorithme de Lenstra-Lenstra-Lovász de réduction de base de lattice (LLL-algorithme) que nous décrivons ci-dessous. Soit $\tau_1, \tau_2, \ldots, \tau_t \in \mathbb{R}$ et la forme linéaire

$$x_1\tau_1 + x_2\tau_2 + \cdots + x_t\tau_t \quad \text{avec} \quad |x_i| \leq X_i. \tag{3.8}$$

On pose $X := \max\{X_i\}$, $C > (tX)^t$ et considérons le lattice entier Ω engendré par :

$$b_j := e_j + \lfloor c\tau_j \rceil \quad \text{pour} \quad 1 \leq j \leq t-1 \quad \text{et} \quad b_t := \lfloor C\tau_t \rceil e_t,$$

où C est une constante positive suffisamment grande.

Lemme 3.2.5 (LLL-algorithme)**.**
Soient $X_1, X_2, \cdots, X_t$ des entiers positifs tels que $X := \max\{X_i\}$ et $C > (tX)^t$ est une constante positive fixée suffisamment grande. Avec les notations ci-dessus sur le lattice Ω, nous considérons une base réduite b_i à Ω et sa base d'orthogonalisation de Gram-Schmidt associée $\{b_i^*\}$. Nous fixons

$$c_1 := \max_{1\leq i\leq t} \frac{\|b_1\|}{\|b_i^*\|}, \quad \theta := \frac{\|b_1\|}{c_1}, \quad Q := \sum_{i=1}^{t-1} X_i^2, \quad et \quad R := \frac{1}{2}\left(1 + \sum_{i=1}^{t} X_i\right).$$

Si les entiers x_i sont tels que $|x_i| \leq X_i$, pour $1 \leq i \leq t$ et $\theta^2 \geq Q + R^2$, alors nous avons

$$\left|\sum_{i=1}^{t} x_i\tau_i\right| \geq \frac{\sqrt{\theta^2 - Q} - R}{C}.$$

Pour la preuve et plus de détails, nous référons le lecteur au livre de Cohen. (Proposition 2.3.20 dans [43], pp. $58-63$).

Dans les sections suivantes, nous allons utiliser les formes linéaires de logarithmes énoncées plus haut pour résoudre des équations Diophantiennes exponentielles en suites récurrentes linéaires.

3.3 Puissances de trois comme différence de deux nombres de Fibonacci

Cette section est une version légèrement modifiée d'un article intitulé *Powers of Three as Difference of Two Fibonacci Numbers*, publié en Février 2021 dans **JP Journal of Algebra, Number Theory and Applications**, Volume 49, Number 2, (2021), Pages $185-196$.

Résumé : Le but de cet article est de trouver, de manière simple et rigoureuse, toutes les puissances de trois qui peuvent être représentées comme différence de deux nombres de Fibonacci, c'est-à-dire que nous étudions l'équation Diophantienne exponentielle $F_n - F_m = 3^p$. Nous déterminons toutes les solutions entières positives n, m, et p où $(F_n)_{n\geq 0}$ est la suite de Fibonacci. Les outils utilisés pour résoudre notre résultat principal sont les propriétés des fractions continues, les formes linéaires de logarithmes, et une version de la méthode de réduction de Baker-Davenport en approximation Diophantienne.

3.3.1 Introduction

Les nombres de Fibonacci et Lucas $1, 1, 2, 3, 5, 8, \ldots$ et $2, 1, 3, 4, 7, 11, \ldots$ ont depuis des centaines d'années fasciné certains mathématiciens. Les suites de Fibonacci et de Lucas sont définies récursivement par $F_n = F_{n-1} + F_{n-2}$ pour $n \geq 2$. Elles sont générées par $F_0 = 1, \quad F_1 = 1$ et $F_0 = 2, \quad F_1 = 1$ respectivement. La détermination des puissances parfaites des suites de Lucas et de Fibonacci ne date pas d'aujourd'hui. Elles ont de nombreuses propriétés intéressantes et ont été étudiés par de nombreux chercheurs. Pour un bref historique des suites de Fibonacci et de Lucas, on peut faire référence à [34]. Les propriétés des suites de Fibonacci et de Lucas, et la relation entre elles, ont fait l'objet d'un nombre considérable de recherches. L'apport réel de la détermination des puissances parfaites des suites de Lucas et de Fibonacci a commencé en 2006. Par des approches classiques et modulaires des équations Diophantiennes, Bugeaud, Mignotte et Siksek [37] déterminaient toutes les puissances parfaites des suites de Lucas et de Fibonacci en résolvant les équations $L_n = y^p$ and $F_n = y^p$.

Tout d'abord, les carrés parfaits et plus tard les puissances parfaites des suites de Fibonacci et de Lucas ont attiré l'attention des chercheurs. À partir de là, de nombreux chercheurs ont abordé des problèmes similaires.

Dans le corollaire 1 de [24], S. Kebli, O. Kihel, J. Larone, et F. Luca donnent la condition sur toutes les solutions entières de l'équation $F_n \pm F_m = y^a$. Ils ont aussi montré dans les Théorèmes 1 et 2 de [24] les conditions que l'équation $F_n \pm F_m = y^a$ doit satisfaire pour avoir un nombre fini de solutions entières positives (n, m, y, a). La preuve de leur théorème 2 est basée sur la conjecture *abc* (problème ouvert). Mais ils utilisent également une borne supérieure sur $n - m$ qui apparaît dans la preuve de théorème 1 de [24] et repose sur une application de bornes inférieures pour les formes linéaires de logarithmes des nombres algébriques. On peut consulter [24] pour plus d'informations. Nos résultats respectent toutes les conditions données en [24].

Motivés par les récentes études de Bravo et Luca [24, 25], notre objectif principal est de déterminer les puissances de 3 qui peuvent être représentées comme différence de deux nombres de Fibonacci.

Nous considérons l'équation Diophantienne :

$$F_n - F_m = 3^p \tag{3.9}$$

avec pour inconnues les entiers positifs m, n, et p. Nous suivons l'approche et la méthode présentées par Luca et Bravo dans [25]. La preuve de notre résultat principal utilise les bornes inférieures sur les formes linéaires de logarithmes, les propriétés des fractions continues et une version de la méthode de réduction de Baker-Davenport en approximation Diophantienne.

Cet article suit les étapes suivantes : dans la section 3.3.2, nous introduisons les théorèmes nécessaires et lemme qui sera utilisé dans les sections suivantes pour prouver le résultat principal de cette section. Nous énonçons et prouvons le théorème suivant :

Théorème 3.3.1.
Les seules solutions entières positives (n, m, p) *de l'équation Diophantienne* $F_n - F_m = 3^p$ $m < n$ *et* $p \geq 0$ *sont*

$$(1,0,0), \quad (2,0,0), \quad (3,1,0), \quad (3,2,0), \quad (4,0,1), \quad (4,3,0), \quad (5,3,1), \quad (6,5,1), \quad (11,6,4).$$

3.3.2 Résultats auxiliaires

Dans cette section, nous rappelons quelques résultats importants qui nous seront utiles pour atteindre notre objectif. Les formules de Binet bien connues, qui fournissent des règles pour calculer les nombres de Fibonacci et de Lucas. Les deux incorporent le soi-disant nombre d'or $(1+\sqrt{5})/2$, faisant allusion à une profonde connexion entre les suites :

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} \quad \text{et} \quad L_n = \alpha^n + \beta^n$$

où $\alpha = (1+\sqrt{5})/2$ et $\beta = (1-\sqrt{5})/2$ sont les racines de l'équation caractéristique $x^2 - x - 1 = 0$. La relation entre les nombres de Fibonacci et α est :

$$F_{n+1} + F_{n-1} = L_n, \quad \text{pour} \quad n \geq 1. \tag{3.10}$$

$$\alpha^{n-2} \leq F_n \leq \alpha^{n-1}, \quad \text{pour} \quad n \geq 1. \tag{3.11}$$

L'équation (3.11) peut être prouvée facilement par induction. En associant les équations (3.11) et (3.10) nous allons dans la section suivante prouver l'inégalité importante suivante : $1 \leq p < n$. Il peut être remarqué que $1 < \alpha < 2$ et $-1 < \beta < 0$.

Le théorème suivant dû à Luca et Patel est donné dans [28].

Théorème 3.3.2 (F. Luca et V. Patel)**.**
Toutes les solutions entières (n, m, y, p) *de l'équation Diophantienne* $F_n \pm F_m = y^p, \quad p \geq 2$ *avec* $n \equiv m \pmod 2$ *ont soit* $\max\{|n|, |m|\} < 36$ *ou* $y = 0$ *et* $|n| = |m|$.

Le théorème 3.3.2 est une généralisation du théorème suivant dû à Bugeaud, Luca, Mignotte et Siksek [37].

Théorème 3.3.3.
Les seules solutions entières positives (n, y, p) *de l'équation* $F_n - 1 = y^p$ *avec* $p \geq 2$ *sont*

$$F_1 - 1 = F_2 - 1 = 0, \quad F_3 - 1 = 1, \quad F_5 - 1 = 2^2.$$

3.3.3 Résultat principal

Dans cette section, nous donnons la preuve du théorème 3.3.1.

Démonstration.
Admettons que l'équation

$$F_n - F_m = 3^p \tag{3.12}$$

est vérifiée.

Si $m = 0$, (3.9) devient $F_n = 3^p$, les seules solutions (n, m, p) sont $(1, 0, 0)$, $(2, 0, 0)$ et $(4, 0, 1)$, et $n \leq 12$ d'après le Théorème 2 dans [28].

Si $m = 1$ ou 2, alors nous avons l'équation $F_n - 1 = 3^p$. D'après le théorème 3.3.3, nous avons

$$(n, m, p) \in \{(3, 1, 0), (3, 2, 0)\}.$$

Maintenant, supposons que $n - m \in \{1, 2\}$. Alors (3.9) devient $3^p = F_{n-2}$ pour $m = n - 1$ ou $3^p = F_{n-1}$ pour $m = n - 2$. D'après [28], nous avons $(n, m, p) = (2, 0, 0), (3, 1, 0), (3, 2, 0), (4, 3, 0), (5, 3, 1), (6, 5, 1)$. Grâce à *Mathematica*, nous obtenons les solutions énoncées dans le théorème principal pour $1 \leq m < n \leq 200$.

Maintenant, supposons que $n > 200, \quad m \geq 3 \quad$ et $\quad m - n \geq 3$. Nous allons prouver une importante inégalité. De $\alpha^{n-2} \leq F_n \leq \alpha^{n-1}$, on obtient

$$3^p = F_n - F_m < F_n < \alpha^n < 3^n \quad \text{c'est-à-dire} \quad 3^p < 3^n. \tag{3.13}$$

Vu que $m > 3$ et $n - m \geq 3$, il s'ensuit que :

$$3^p = F_n - F_m \geq F_{m+3} - F_m = 2F_{m+1} \geq 6. \tag{3.14}$$

De (3.13) et (3.14), on obtient $1 \leq p < n$.

Maintenant, supposons que $n \equiv m \pmod 2$. Ce cas a été complètement résolu par Lucas et Patel [28], et ils ont obtenu $n \leq 36$. Ceci contredit notre supposition $n > 200$. Ainsi (3.9) n'a aucune solution quand n et m ont les mêmes parités.

Nous supposons maintenant que n et m sont de différentes parités.

$$F_n - F_m = 3^p \Longrightarrow \left|\frac{\alpha^n}{\sqrt{5}} - 3^p\right| = \left|F_m + \frac{\beta^n}{\sqrt{5}}\right| < \alpha^m + \frac{\beta^n}{\sqrt{5}} < \alpha^m + \frac{1}{2}$$

Divisant les deux membres par $\frac{\alpha^n}{\sqrt{5}}$, on obtient

$$\left|1 - 3^p\sqrt{5}\alpha^{-n}\right| < 4/\alpha^{n-m} \tag{3.15}$$

Maintenant, appliquons le théorème de Matveev avec les données suivantes :

$$\gamma_1 := 3, \quad \gamma_2 := \alpha, \quad \gamma_3 := \sqrt{5}, \quad b_1 := p, \quad b_2 := -n, \quad \text{et} \quad b_3 := 1.$$

Puisque $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Q}(\sqrt{5})$. Donc, nous pouvons prendre $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Ainsi, $D = \deg(x^2 - 5) = 2$. $\Lambda_1 = 3^p\sqrt{5}\alpha^{-n} - 1$ est non nul. Autrement, nous obtenons

$$3^p = \frac{\alpha^p}{\sqrt{5}} = F_n + \frac{|\beta|^n}{\sqrt{5}} > F_n - 1 > F_n - F_m = 3^p \quad \text{qui est impossible.}$$

Nous pouvons prouver que Λ_1 différent de zéro en utilisant le conjugué de $3^p = \frac{\alpha^p}{\sqrt{5}}$.

En outre $h(\gamma_1) = \log 3, \quad h(\gamma_2) = \frac{1}{2}\log\alpha, \quad h(\gamma_3) = \log\sqrt{5}$. Alors nous pouvons prendre, $A_1 = 2.2, \quad A_2 = 0.5, \text{et} \quad A_3 = 1.7$. Puisque $p < n$, il s'ensuit que $B := \max\{|p|, |-n|, 1\} = n$. Puisque toutes les conditions sont réunies pour appliquer le Théorème 3.2.6, nous avons

$$\frac{4}{\alpha^{n-m}} > |\Lambda_1| > \exp\left(-1.4 \times 30^6 \times 3^{4.5} \times 2^2(1 + \log 2)(1 + \log n) \times 2.2 \times 0.5 \times 1.7\right)$$

ainsi

$$(n-m)\log\alpha - \log 4 < 1.4\times 30^6\times 3^{4.5}\times 2^2(1+\log 2)(1+\log n)\times 2.2\times 0.5\times 1.7$$

et un calcul rapide dans *Mathematica* donne pour

$$(n-m)\log\alpha < 2.16\times 10^{12}(1+\log n) < 3.6\times 10^{16}\log n. \tag{3.16}$$

où nous avons utilisé l'inégalité $1+\log n < 2\log n$ qui est vérifiée pour tout $n \geq 3$. Dans le but de trouver la borne de n, réécrivons l'équation (3.9) et appliquons le théorème de Matveev une seconde fois.

$$F_n - F_m = 3^p \Longrightarrow \frac{\alpha^n(1-\alpha^{m-n})}{\sqrt{5}} - 3^p = \frac{\beta^n-\beta^m}{\sqrt{5}}.$$

En prenant entre valeurs absolues l'équation précédente et en utilisant le fait que $|\beta|^n + |\beta|^m < \frac{2}{3}; n > 200$; nous obtenons

$$\left|\frac{\alpha^n\left(1-\alpha^{m-n}\right)}{\sqrt{5}} - 3^p\right| \leq \frac{|\beta|^n+|\beta|^m}{\sqrt{5}} < \frac{1}{3}$$

ainsi

$$\left|1 - 3^p\sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}\alpha^{-n}\right| < 3/\alpha^n \tag{3.17}$$

parce que

$$\alpha^{m-n} = \frac{1}{\alpha^{n-m}} < \frac{1}{\alpha} < \frac{2}{3} \Longrightarrow 1-\alpha^{m-n} > \frac{1}{3} \Longrightarrow \left(1-\alpha^{m-n}\right)^{-1} < 3$$

De (3.17), en prenant $\gamma_1 := 3, \quad \gamma_2 := \alpha, \quad \gamma_3 := \sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}; \quad b_1 := p, \quad b_2 := -n,$ $b_3 := 1$. Puisque $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Q}(\sqrt{5})$. Nous pouvons prendre $\mathbb{K} = \mathbb{Q}(\sqrt{5})$. Ainsi, $D = \deg(x^2-5) = 2$. $\Lambda_2 := 3^p\sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}\alpha^{-n} - 1$. Prouvons que $\Lambda_2 \neq 0$ par contradiction. Si $\Lambda_2 = 0$, alors, nous avons

$$3^p = \frac{\alpha^n-\alpha^m}{\sqrt{5}} \Longrightarrow \frac{\beta^n}{\sqrt{5}} = \frac{\beta^m}{\sqrt{5}} \quad \text{qui est impossible vu que} \quad n > m.$$

De même, $h(\gamma_1) = \log 3, \quad h(\gamma_2) = \frac{1}{2}\log\alpha, \quad h(\gamma_3) \leq \log 2\sqrt{5} + \frac{1}{2}(n-m)\log\alpha$ ainsi, nous pouvons prendre $A_1 = 2.2, \quad A_2 = 0.5, \quad A_3 = \log 20 + (n-m)\log\alpha$. Aussi, vue que $p < n$,

alors $B := \{p, |-n|, 1\} = n$. Ce qui implique que

$$\frac{3}{\alpha^n} > |\Lambda_2| > \exp\left((-C)(1+\log 2)(1+\log n)\cdot 2.2\cdot 0.5\cdot(\log 20 + (n-m)\log\alpha)\right)$$

ou

$$n\log\alpha - \log 3 < C(1+\log 2)(1+\log n)\cdot 2.2\cdot 0.5\cdot(\log 20 + (n-m)\log\alpha) \tag{3.18}$$

où $C = 1.4\cdot 30^6\cdot 3^{4.5}\cdot 2^2$. En remplaçant (3.16) dans (3.18), on obtient

$$n\log\alpha - \log 3 < C(1+\log 2)(1+\log n)\times 2.2\times 0.5\times(\log 20 + 3.6\times 10^{16}\log n)$$

et $n < 4.6\times 10^{32}$. Notre objectif est de réduire à présent cette borne supérieure sur n. Pour cela, appliquons le Lemme de Dujella et Pethő. De (3.15), soit

$$z_1 := p\log 3 - n\log\alpha + \log\sqrt{5}.$$

Alors $|1-e^{z_1}| < 4/\alpha^{n-m}$ grâce à (3.16). L'inégalité

$$\frac{\alpha^n}{\sqrt{5}} = F_n + \frac{\beta^n}{\sqrt{5}} > F_n - 1 > F_n - F_m = 3^p$$

implique que $z_1 < 0$. Dans ce cas, vu que $4/\alpha^{n-m} < 0.95$ pour $n-m \geq 3$, il s'ensuit que $e^{|z_1|} < 20$, on obtient

$$0 < |z_1| < e^{|z_1|} - 1 \leqslant e^{|z_1|}|1-e^{z_1}| < 80/\alpha^{n-m}$$

ou

$$0 < |p\log 3 - n\log\alpha + \log\sqrt{5}| < 80/\alpha^{n-m}$$

alors, en divisant cette précédente équation par $\log\alpha$, obtient

$$0 < \left| p\left(\frac{\log 3}{\log\alpha}\right) - n + \frac{\log\sqrt{5}}{\log\alpha}\right| < 167\cdot\alpha^{-(n-m)}$$

Appliquons à présent le lemme de Dujella et Pethő avec les données suivantes : Il est clair que $\gamma := \dfrac{\log 3}{\log\alpha}$ est irrationnel.

Soit $\mu := \dfrac{\log\sqrt{5}}{\log\alpha}$, $A := 167$, $B := \alpha$, $k := n-m$. Prenons $M := 4.6 \times 10^{32}$, nous obtenons après calcul dans *SageMath*, $q_{65} = 1431273036226644731402283420922554 3 > 6M$ et

$$n - m \leq \frac{\log(Aq_{65}/\epsilon)}{\log B} < 84.7638$$

. On obtient $n - m < 85$.

En remplaçant cette borne supérieure par $n - m$ dans (3.18), on obtient $n < 3.58 \times 10^{15}$.

Maintenant, de (3.17), soit $z_2 = p\log 3 - n\log\alpha + \log\left(\sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}\right)$. Dans ce cas,

$$|1 - e^{z_2}| < 3/\alpha^n.$$

Il apparaît que $3/\alpha^n < 1/2$. Deux cas se présentent : lorsque $z_2 > 0$ et $z_2 < 0$.

- **Cas 1 :** $z_2 > 0$

  Alors $0 < z_2 < e^{z_2} - 1 < 3/\alpha^n$

- **Cas 2 :** $z_2 < 0$

  Alors $|1 - e^{z_2}| = 1 - e^{z_2} < 3/\alpha^n < 1/2 \Longrightarrow e^{z_2} < 2$ et donc

  $$0 < |z_2| < e^{z_2} - 1 = e^{|z_2|}|1 - e^{z_2}| < 6/\alpha^n \Longrightarrow 0 < |z_2| < 6/\alpha^n$$

  qui est équivalent à

  $$0 < \left|p\log 3 - n\log\alpha + \log\left(\sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}\right)\right| < 6/\alpha^n$$

  donc

  $$0 < \left|p\frac{\log 3}{\log\alpha} - n + \frac{\log\left(\sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}\right)}{\log\alpha}\right| < 13\cdot\alpha^n.$$

  En mettant $\gamma = \dfrac{\log 3}{\log\alpha}$; et en prenant $M = 3.58 \times 10^{15}$; nous obtenons avec $\mu = \dfrac{\log\left(\sqrt{5}\left(1-\alpha^{m-n}\right)^{-1}\right)}{\log\alpha}$, pour $n - m \in [3, 84]$, $A = 13$, $B = \alpha$, $k = n$ grâce au lemme 3.2.4, que $q_{40} = 4488642667247434242$ et donc $n \leq \dfrac{\log\left(Aq_{40}/\epsilon\right)}{\log B} \leq 80$.

Ceci contredit notre hypothèse $n > 200$. Ce qui termine la preuve de notre théorème principal. □

3.4 Sur les solutions de l'équation Diophantienne

$$L_n + L_m = 3^a$$

Cette section est une version légèrement modifiée d'un article intitulé *On solutions of the Diophantine equation* $L_n + L_m = 3^a$, publié dans **Malaya J. Mat.** 9 (04) (2021), 228 − 238.

Résumé : Soit $(L_n)_{n\geq 0}$ la suite de Lucas donnée par $L_0 = 2, L_1 = 1$ et $L_{n+2} = L_{n+1} + L_n$ pour $n \geq 0$. Dans cet article, nous nous intéressons à trouver toutes les puissances de trois qui sont somme de deux nombres de Lucas. En d'autres termes, nous étudions l'équation Diophantienne exponentielle $L_n + L_m = 3^a$ d'inconnus, les entiers positifs n, m, et a. La preuve de notre théorème principal utilise des bornes inférieures pour les formes linéaires de logarithmes, les propriétés des fractions continues et une version de la méthode de réduction de Baker-Davenport en approximation Diophantienne.

3.4.1 Introduction

La détermination des puissances parfaites des suites de Lucas et de Fibonacci ne date pas d'aujourd'hui. La véritable contribution de la détermination des puissances parfaites des suites de Lucas et Fibonacci a commencée en 2006. Par des approches classiques et modulaires des équations Diophantiennes, Bugeaud, Mignotte et Siksek [27] ont déterminé toutes les puissances parfaites des suites de Lucas et Fibonacci en résolvant respectivement les équations $F_n = y^p$ et $L_n = y^p$. À partir de là, de nombreux chercheurs se sont attaqués à des problèmes similaires. C'est dans la même pensée que, d'autres ont déterminé les puissances de 2 de la somme/différence de deux nombres de Lucas, puissances de 2 ou puissances parfaites de la somme/différence de nombres de Fibonacci [24, 28] [25], puissances de 2 et de 3 du produit des nombres de Pell et des nombres de Fibonacci.

Au regard de ce qui a été fait, nous avons décidé de nous intéresser aux puissances de 3 qui peuvent être représentées comme somme de deux nombres de Lucas. Cet article suit les étapes suivantes : Nous donnons d'abord les généralités sur les suites récurrentes linéaires binaires, puis nous démontrons une inégalité importante sur les nombres de Lucas et enfin déterminons et réduisons une borne grossière. La dernière section de ce chapitre est consacrée à la réduction de la borne grossière obtenue et à la discussion des différents cas possibles. On sait par Bravo et Luca [41] que les seules solutions de l'équation Diophantienne

$F_n + F_m = 2^a$ d'inconnus, les entiers positifs n, m et a avec $n \geq m$ sont données par

$$2F_1 = 2, \quad 2F_2 = 2, \quad 2F_3 = 4, \quad 2F_6 = 16,$$

et

$$F_2 + F_1 = 2, \quad F_4 + F_1 = F_4 + F_2 = 4, \quad F_5 + F_4 = 8, \quad F_7 + F_4 = 16.$$

et dans [25] que toutes les solutions positives entières de l'équation Diophantienne $L_n + L_m = 2^a$ avec $n \geq m$ et a, sont

$$2L_0 = 4, \quad 2L_1 = 2, \quad 2L_3 = 8, \quad L_2 + L_1 = 4, \quad L_4 + L_1 = 8, \quad \text{et} \quad L_7 + L_2 = 32.$$

Dans cet article, nous déterminons toutes les solutions positives entières de l'équation Diophantienne exponentielle suivante :

$$L_n + L_m = 3^a \tag{3.19}$$

avec $n \geq m$ et a.

3.4.2 Inégalités impliquant les nombres de Lucas

Dans cette section, nous énonçons et prouvons des inégalités importantes associées aux nombres de Lucas qui seront utilisés pour résoudre l'équation (3.19).

Proposition 3.4.1.

Pour $n \geq 2$, nous avons

$$0.94\,\alpha^n < (1 - \alpha^{-6})\alpha^n \leq L_n \leq (1 + \alpha^{-4})\alpha^n < 1.15\,\alpha^n \tag{3.20}$$

Démonstration.

Cela découle directement de la formule $L_n = \alpha^n + (-1)^n \alpha^{-n}$. □

3.4.3 Résultat principal

Notre résultat principal peut être énoncé sous forme de théorème comme suit :

Théorème 3.4.1.

Les seules solutions (n, m, a) positives entières de l'équation Diophantienne exponentielle

$L_n + L_m = 3^a$ avec $n \geq m$ et a, sont : $(1,0,1) \quad et \quad (4,0,2)$

$$i.e \quad L_1 + L_0 = 3, \quad et \quad L_4 + L_0 = 9.$$

Démonstration.

D'abord, nous étudions le cas $n = m$, ensuite nous supposons $n > m$ et examinons le cas $n \leq 200$ avec *SageMath* dans la gamme $0 \leq m < n \leq 200$ et enfin nous considérons le cas $n > 200$. Supposons que cette équation (3.19) soit vérifiée. Tout d'abord, remarquons que si $n = m$, alors l'équation originale (3.19) devient

$$L_n = \frac{3^a}{2}.$$

Cette équation n'a pas de solution car , $\forall n > 0, L_n \in \mathbb{Z}$. Donc à partir de maintenant, nous supposons $n > m$.

Si $n \leq 200$, la recherche avec *SageMath* dans l'intervalle $0 \leq m < n \leq 200$ donne les solutions $(n, m, a) \in \{(1,0,1), (4,0,2)\}$. Dès lors, pour le reste de l'article, nous supposons $n > 200$. Déterminons d'abord une relation entre a et n qui est importante pour la suite. En combinant (3.19) et l'inégalité de droite de (3.20), on obtient :

$$3^a = L_n + L_m \leq 2\alpha^n + 2\alpha^m < 2^{n+1} + 2^{m+1} = 2^{n+1}(1 + 2^{n-m}) \leq 2^{n+1}(1 + 1/2) < 2^{n+2}.$$

En prenant log des deux côtés, on obtient

$$a \log 3 \leq (n+2) \log 2 \Longrightarrow a \leq (n+2)c_1 \quad \text{où} \quad c_1 = \frac{\log 2}{\log 3}.$$

Réécrivant (3.19) comme :

$$L_n + L_m = \alpha^n + \beta^n + L_m = 3^a \Longrightarrow \alpha^n - 3^a = -\beta^n - L_m.$$

En appliquant les valeurs absolues des deux côtés, on obtient

$$|\alpha^n - 3^a| = |\beta^n + L_m| \leq |\beta|^n + L_m < \frac{1}{2} + 2\alpha^m \quad \because |\beta|^n < \frac{1}{2}, \quad \text{et} \quad L_m < 2\alpha^m.$$

En divisant les deux membres de l'équation précédente par α^n et en considérant le fait que

$n > m$, on obtient :

$$\left|1 - \alpha^{-n} \cdot 3^a\right| < \frac{\alpha^{-n}}{2} + 2\alpha^{m-n} < \frac{1}{\alpha^{n-m}} + \frac{2}{\alpha^{n-m}} \quad \because \frac{1}{2\alpha^n} < \frac{1}{\alpha^{n-m}}; \quad n > m$$

d'où

$$\left|1 - \alpha^{-n} \cdot 3^a\right| < \frac{3}{\alpha^{n-m}} \tag{3.21}$$

Prenons

$$\gamma_1 := \alpha, \quad \gamma_2 := 3, \quad b_1 := n, \quad b_2 := a, \quad \Gamma := a\log 3 - n\log\alpha$$

afin d'appliquer le théorème 3.2.8. Par conséquent, l'équation (3.21) peut être réécrite comme :

$$\left|1 - e^{\Gamma}\right| < \frac{3}{\alpha^{n-m}} \quad \text{où} \quad e^{\Gamma} = \alpha^{-n}3^a. \tag{3.22}$$

Puisque $\mathbb{Q}(\sqrt{5})$ est le corps de nombres algébriques contenant γ_1, γ_2 ; donc on peut prendre $D := 2$. En utilisant l'équation (3.19) et la formule de Binet pour la suite de Lucas, nous avons :

$$\alpha^n = L_n - \beta^n < L_n + 1 \leq L_n + L_m = 3^a$$

ce qui implique $1 < 3^a\alpha^{-n}$ et donc $\Gamma > 0$. En combinant cela avec (3.22), nous obtenons

$$0 < \Gamma < \frac{3}{\alpha^{n-m}} \tag{3.23}$$

où nous avons utilisé le fait que $x \leq e^x - 1, \quad \forall x \in \mathbb{R}$. En appliquant log à droite et à gauche de (3.23), on a

$$\log\Gamma < \log 3 - (n-m)\log\alpha. \tag{3.24}$$

La hauteur logarithmique de γ_1 et γ_2 sont :

$h(\gamma_1) = \frac{1}{2}\log\alpha = 0.2406\cdots$, $h(\gamma_2) = \log 3 = 1.09862\cdots$, ainsi on peut choisir

$$\log A_1 := 0.5 \quad \text{and} \quad \log A_2 := 1.1.$$

Enfin, en rappelant que $a \leq (n+2)c_1; \quad c_1 = 0.63093$, on obtient :

$$b' := \frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1} = \frac{n}{2.2} + a = 0.45n + a < 0.45n + (n+2)c_1 < 2n.$$

Il est facile de voir que α et 3 sont multiplicativement indépendants. Alors d'après le théorème 3.2.8, on a

$$\log \Gamma \geq -30.9 \cdot 2^4 \left(\max \left\{ \log(2n), \frac{21}{2}, \frac{1}{2} \right\} \right)^2 \cdot 0.5 \cdot 1.1$$

$$\log \Gamma > -272 \left(\max \left\{ \log(2n), \frac{21}{2}, \frac{1}{2} \right\} \right)^2. \tag{3.25}$$

En combinant les équations (3.24) et (3.25), on obtient cet important résultat suivant

$$(n-m) \log \alpha < 276 \left(\max \left\{ \log(2n), \frac{21}{2}, \frac{1}{2} \right\} \right)^2. \tag{3.26}$$

Trouvons une seconde forme linéaire de logarithme. Pour cela, nous réécrivons (3.19) comme suit :

$$\alpha^n (1 + \alpha^{n-m}) - 3^a = -\beta^n - \beta^m.$$

En prenant en valeurs absolues la relation ci-dessus, on obtient

$$|\alpha^n (1 + \alpha^{m-n}) - 3^a| < 2, \quad \beta = (1 - \sqrt{5})/2, \quad |\beta|^n < 1 \quad \text{et} \quad |\beta|^m < 1; \forall n > 200, \quad m \geq 0.$$

En divisant les deux membres de l'inégalité ci-dessus par $\alpha^n (1 + \alpha^{m-n})$, on obtient

$$\left| 1 - 3^a \alpha^{-n} (1 + \alpha^{m-n})^{-1} \right| < \frac{2}{\alpha^n} \quad \text{i.e} \quad |\Lambda| < \frac{2}{\alpha^n}. \tag{3.27}$$

Toutes les conditions sont maintenant réunies pour appliquer le théorème de Matveev (Théorème 3.2.6).

- Données :

$$t := 3; \quad \gamma_1 := 3; \quad \gamma_2 := \alpha; \quad \gamma_3 := 1 + \alpha^{m-n}$$

$$b_1 := a; \qquad b_2 := -n, \quad b_3 = -1.$$

Comme précédemment, $\mathbb{K} = \mathbb{Q}(\sqrt{5})$ contient $\gamma_1, \gamma_2, \gamma_3$ et a $D := [\mathbb{K} : \mathbb{Q}] = 2$. Avant de continuer les calculs, vérifions si $\Lambda \neq 0$.

$\Lambda \neq 0$ vient du fait que s'il était nul, on aurait

$$3^a = \alpha^n + \alpha^m \tag{3.28}$$

En prenant le conjugué de la relation ci-dessus dans le corps $\mathbb{Q}(\sqrt{5})$, on obtient :

$$3^a = \beta^n + \beta^m. \tag{3.29}$$

En combinant (3.28) et (3.29), on obtient :

$$\alpha^n < \alpha^n + \alpha^m = |\beta^n + \beta^m| \leq |\beta|^n + |\beta|^m < 2.$$

Rappelons que $n > 200$. Cette relation est impossible pour $n > 200$. D'où $\Lambda \neq 0$.

- **Calculs de** $h(\gamma_3)$

  Estimons maintenant $h(\gamma_3)$ où $\gamma_3 = 1 + \alpha^{m-n}$

$$\gamma_3 = 1 + \alpha^{m-n} < 2 \quad \text{et} \quad \gamma^{-1} = \frac{1}{1+\alpha^{m-n}} < 1$$

  ainsi $|\log \gamma_3| < 1$. Notons que

$$h(\gamma_3) \leq |m-n| \left(\frac{\log \alpha}{2}\right) + \log 2 = \log 2 + (n-m)\left(\frac{\log \alpha}{2}\right).$$

- Le calcul de A_1 et A_2 donne :

$$A_1 := 2.2$$

  et

$$A_2 := 0.5$$

  et nous pouvons prendre

$$A_3 := 2 + (n-m)\log \alpha \quad \text{vu que} \quad h(\gamma_3) := \log 2 + (n-m)\left(\frac{\log \alpha}{2}\right)$$

- **Calcul de** B

Puisque $a < (n+2)c_1$, il s'ensuit que, $B = \max\{1, n, a\}$. On peut donc prendre $B = n+1$.

En remplaçant les données, le théorème de Matveev donne la borne inférieure du côté gauche de (3.27).

$$\exp\left(-C(1+\log(n+1))\cdot 2.2\cdot 0.5\cdot(2+(n-m)\log\alpha)\right)$$

où

$$C := 1.4\cdot 30^6\cdot 3^{4.5}\cdot 2^2(1+\log 2) < 9.7\times 10^{11}.$$

En remplaçant dans l'équation (3.27), on obtient :

$$\exp\left(-C(1+\log(n+1))\cdot 2.2\cdot 0.5\cdot(2+(n-m)\log\alpha)\right) < |\Lambda| < \frac{2}{\alpha^n}$$

qui conduit à

$$n\log\alpha - \log 2 < C((1+\log(n+1))\cdot 1.1\cdot(2+(n-m)\log\alpha) < 2C\log n\cdot 1.1\cdot(2+(n-m)\log\alpha)$$

alors

$$n\log\alpha - \log 2 < 1.26\times 10^{12}\log n\cdot(2+(n-m)\log\alpha) \tag{3.30}$$

où nous avons utilisé l'inégalité $1+\log(n+1) < 2\log n$, qui est valable pour $n > 200$.

En utilisant (3.26) dans le terme de droite de l'inégalité ci-dessus (3.30) et en effectuant les calculs associés, nous obtenons

$$n < 7.3\times 10^{14}\log n\left(\max\left\{\log(2n), \frac{21}{2}\right\}\right)^2. \tag{3.31}$$

Si $\max\{\log(2n), 21/2\} = 21/2$, il découle de (3.31) que $n < 8.04825\cdot 10^{16}\log n \implies n < 3.5\cdot 10^{18}$. D'autre part, si $\max\{\log(2n), 21/2\} = \log(2n)$, alors de (3.31), on a $n < 7.3\cdot 10^{14}\log n\log^2(2n)$ et donc $n < 7.2\cdot 10^{19}$. On voit facilement que pour les deux valeurs possibles de $\max\{\log(2n), 21/2\}$, on a $n < 7.2\cdot 10^{19}$.

Tous les calculs effectués jusqu'à présent peuvent être résumés dans le lemme suivant.

Lemme 3.4.1.

Si (n, m, a) est une solution de (3.19) avec les conditions $n > m$ et $n > 200$, alors les inégalités

$$a \leq n + 2 < 1.2 \times 10^{20} \quad \textit{sont vérifiées.}$$

3.4.4 Réduction de la borne sur n

En divisant l'inégalité (3.23) : $0 < a\log 3 - n\log\alpha < \dfrac{3}{\alpha^{n-m}}$ par $\log\alpha$, on obtient

$$0 < a\gamma - n < \frac{7}{\alpha^{n-m}}; \quad \text{où} \quad \gamma := \frac{\log 3}{\log\alpha}. \tag{3.32}$$

La fraction continue du nombre irrationnel γ est :

$$[a_0, a_1, a_2, ...] = [1, 2, 3, 1, 1, 2, 3, 2, 4, 2, 1, 11, 2, 1, 11, ...]$$

et notons p_k/q_k son convergent. Une inspection utilisant *SageMath* donne l'inégalité suivante

$$4977896525362041575 = q_{41} < 1.2 \times 10^{20} < q_{42} = 805929983250536127817.$$

De plus, $a_M := \max\{a_i | i = 0, 1, ..., 42\} = 161$ En appliquant maintenant le lemme 3.2.3 et les propriétés des fractions continues, on obtient

$$|a\gamma - n| > \frac{1}{(a_M + 2)a}. \tag{3.33}$$

Combinant les équations (3.32) et (3.33), on obtient

$$\frac{1}{(a_M+2)a} < |a\gamma - n| < \frac{7}{\alpha^{n-m}} \Longrightarrow \frac{1}{(a_M+2)a} < \frac{7}{\alpha^{n-m}} \Longrightarrow \alpha^{n-m} < 7\cdot(161+2)a < 1.3692\cdot 10^{23}.$$

En appliquant log ci-dessus et en divisant par $\log\alpha$, on obtient :

$$(n-m) \leq \frac{\log(7\cdot 163\cdot a)}{\log\alpha} < 111.$$

Pour améliorer la borne supérieure de n, considérons

$$z := a\log 3 - n\log\alpha - \log\rho(u) \quad \text{où} \quad \rho = 1 + \alpha^{-u}. \tag{3.34}$$

De (3.27), on a

$$|1 - e^z| < \frac{2}{\alpha^n}. \tag{3.35}$$

Puisque $\Lambda \neq 0$, alors $z \neq 0$. Deux cas se présentent : $z < 0$ et $z > 0$. Pour chaque cas, nous appliquerons le lemme 3.2.4.

- **Cas 1 :** $z > 0$

  De (3.35), on obtient $0 < z \leq e^z - 1 < \frac{2}{\alpha^n}$. En remplaçant (3.34) dans l'inégalité ci-dessus, on obtient :

  $$0 < a\log 3 - n\log\alpha - \log\rho(n-m) \leq 3^a\alpha^{-n}\rho(n-m)^{-1} - 1 < 2\alpha^{-n}$$

  d'où

  $$0 < a\log 3 - n\log\alpha - \log\rho(n-m) < 2\alpha^{-n}$$

  et en divisant l'inégalité ci-dessus par $\log\alpha$

  $$0 < a\left(\frac{\log 3}{\log\alpha}\right) - n - \frac{\log\rho(n-m)}{\log\alpha} < 5\cdot\alpha^{-n}. \tag{3.36}$$

  En prenant, $\gamma := \frac{\log 3}{\log\alpha}$, $\mu := -\frac{\log\rho(n-m)}{\log\alpha}$, $A := 5$, $B := \alpha$, l'inégalité (3.36) devient

  $$0 < a\gamma - n + \mu < AB^{-n}.$$

  γ étant irrationnel, nous allons à présent appliquer le lemme 3.2.4 de Dujella et Pethő sur (3.36) pour $n - m \in \{1, ..., 111\}$.

  Puisque $a \leq 1.2 \times 10^{20}$ du lemme 3.4.1, on peut prendre $M = 1.2 \times 10^{20}$, et on obtient

  $$n < \frac{\log(Aq/\varepsilon)}{\log B} \quad \text{où} \quad q > 6M$$

  est le dénominateur du convergent du nombre irrationnel γ tel que $\varepsilon := ||\mu q|| - M||\gamma q|| > 0$. A l'aide de *SageMath*, avec les conditions $z > 0$, et (n, m, a) un possible zéro de (3.19), on obtient $n < 112$. Ceci qui contredit notre hypothèse $n > 200$.

- **Cas 2 :** $z < 0$

  Puisque $n > 200$, alors $\frac{2}{\alpha^n} < \frac{1}{2}$. Par conséquent (3.35) implique que $|1 - e^{|z|}| < 2$. De

plus, puisque $z < 0$, nous avons

$$0 < |z| \leq e^{|z|} - 1 = e^{|z|}|e^{|z|} - 1| < \frac{4}{\alpha^n}.$$

En remplaçant (3.34) dans l'inégalité ci-dessus et en divisant par $\log 3$, on obtient :

$$0 < n\left(\frac{\log \alpha}{\log 3}\right) - a + \frac{\rho(n-m)}{\log 3} < \frac{4}{\log 3} \cdot \alpha^{-n} < 4 \cdot \alpha^{-n} \tag{3.37}$$

Pour appliquer le lemme 3.2.4 sur (3.37) pour $nm \in \{1, 2, ..., 111\}$, reprenons $M = 1,2 \times 10^{20}$. A l'aide de *SageMath*, avec les conditions $z < 0$, et (n, m, a) un possible zéro de (3.19), on obtient $n < 111$ ce qui contredit notre hypothèse $n > 200$.

Ceci termine la preuve de notre résultat principal (théorème 3.4.1).

□

3.5 Sur les solutions de l'équation Diophantienne

$$F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a$$

Cette section est une version développée d'un article intitulé *On solutions of Diophantine equation* $F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a$, publié dans **Journal of Algebra and Related Topics**, Volume 9, Issue 2, 131-148 (2021).

Dans cet article, nous avons déterminé toutes les puissances de 2 qui s'écrivent comme somme de quatre nombres de Fibonacci.

Résumé : Soit $(F_n)_{n\geq 0}$ la suite de Fibonacci donnée par $F_0 = 0, F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour $n \geq 0$. Dans cet article, nous déterminons toutes les puissances de deux qui sont somme de quatre nombres de Fibonacci à quelques exceptions près que nous caractérisons.

3.5.1 Introduction

L'équation $F_n + F_m = y^a$, contrairement à $F_n - F_m = y^a$ a été moins étudiée. Par exemple Z. Siar et R. Keskin [44] ont trouvé toutes les solutions pour $y = 2$, B. Demirtürk et al [45] et P. Tiebekabe et al [46] ont déterminé indépendamment toutes les solutions pour $y = 3$ et enfin F. Erduvan et R. Keskin [47] pour le cas $y = 5$ et ils ont supposé qu'il n'y avait

pas de solutions pour $y > 7$, premier. Concernant les travaux sur la somme des nombres de Fibonacci, le mérite revient à Bravo et Luca [25] qui ont été les premiers à aborder cette équation en résolvant l'équation $F_n + F_m = 2^a$. Le résultat a été généralisé par Pink et Ziegler dans [48]. En 2015, J. Bravo et E. Bravo ont déterminé dans [26] les puissances de 2 qui ont des représentations comme sommes de trois nombres de Fibonacci et dans les commentaires, ils ont espéré qu'il soit possible de venir à bout de l'équation

$$F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a \tag{3.38}$$

avec pour inconnues les entiers positifs n_1, n_2, n_3, n_4 et a avec $n_1 \geqslant n_2 \geqslant n_3 \geqslant n_4$, par la même méthode. Mais le nombre de cas à considérer étant grand, ils laissent cette étude à d'autres chercheurs.

D'autres problèmes similaires à celui discuté dans cet article ont été étudiés pour les suites de Fibonacci et de Lucas. Par exemple, des repdigits qui sont somme d'au plus trois nombres de Fibonacci ont été trouvés dans [29] ; repdigits comme sommes de quatre nombres de Fibonacci ou Lucas ont été trouvés dans [33] ; Les nombres de Fibonacci qui sont somme de deux chiffres repdigits ont été obtenus dans [31], tandis que les factorielles qui sont somme d'au plus trois nombres de Fibonacci ont été trouvées dans [30].

Rappelons que la représentation de Zeckendorf [7] d'un entier positif N est la représentation

$$N = F_{m_1} + F_{m_2} + \ldots + F_{m_t}; \quad \text{avec} \quad m_i - m_{i+1} \geqslant 2 \quad \text{pour} \quad i = 1, \ldots, t-1.$$

L'équation (3.38) est un cas particulier de la représentation de Zeckendorf avec $N = 2^a$ et $t = 4$.

Cet article est subdivisé comme suit : dans la section suivante, nous introduisons les résultats auxiliaires utilisés pour prouver le théorème principal de cet article énoncé ci-dessous.

Théorème 3.5.1 (P. Tiebekabe et I. Diouf)**.**
Toutes les solutions positives entières non nulles n_1, n_2, n_3, n_4 et a de l'équation Diophantienne (3.38) avec $n_1 \geqslant n_2 \geqslant n_3 \geqslant n_4$ sont :

$F_5 + 3F_2 = 2^3$	$F_7 + 3F_2 = 2^4$	$2F_4 + 2F_2 = 2^3$	$F_{13} + F_8 + 2F_2 = 2^8$
$F_4 + 2F_3 + F_2 = 2^3$	$F_6 + F_5 + F_3 + F_2 = 2^4$	$F_8 + F_6 + F_3 + F_2 = 2^5$	$F_{16} + F_9 + F_3 + F_2 = 2^{10}$
$F_{10} + F_5 + F_4 + F_2 = 2^6$	$3F_5 + F_2 = 2^4$	$F_8 + 2F_5 + F_2 = 2^5$	$2F_7 + F_5 + F_2 = 2^5$
$F_9 + F_8 + F_6 + F_2 = 2^6$	$3F_8 + F_2 = 2^6$	$F_{10} + F_5 + 2F_3 = 2^6$	$F_6 + 2F_4 + F_3 = 2^4$
$F_{11} + F_9 + F_4 + F_3 = 2^7$	$F_{13} + F_7 + F_6 + F_3 = 2^8$	$F_{12} + F_{11} + F_8 + F_3 = 2^8$	$F_{12} + 2F_{10} + F_3 = 2^8$
$F_{10} + 3F_4 = 2^6$	$2F_5 + 2F_4 = 2^4$	$F_8 + F_5 + 2F_4 = 2^5$	$2F_7 + 2F_4 = 2^5$
$F_7 + 2F_6 + F_4 = 2^5$	$F_{16} + F_8 + F_7 + F_4 = 2^{10}$	$F_{15} + F_{14} + F_9 + F_4 = 2^{10}$	$F_{13} + F_7 + 2F_5 = 2^8$
$F_{11} + F_8 + F_7 + F_5 = 2^7$	$2F_{10} + F_7 + F_5 = 2^7$	$F_{10} + 2F_9 + F_5 = 2^7$	$F_{16} + F_8 + 2F_6 = 2^{10}$
$F_{11} + 3F_7 = 2^7$	$4F_6 = 2^5$		

3.5.2 Résultat principal

Démonstration.

Supposons que l'équation

$$F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a$$

est vérifiée.

Trouvons d'abord la relation entre n_1 et a.

En combinant l'équation (3.38) avec l'inégalité bien connue $F_n \leqslant \alpha^{n-1}$ pour tout $n \geqslant 1$, on obtient

$$\begin{aligned} F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a \leqslant & \alpha^{n_1-1} + \alpha^{n_2-1} + \alpha^{n_3-1} + \alpha^{n_4-1} \\ < & 2^{n_1-1} + 2^{n_2-1} + 2^{n_3-1} + 2^{n_4-1} \quad \because \alpha < 2 \\ < & 2^{n_1-1}\left(1 + 2^{n_2-n_1} + 2^{n_3-n_1} + 2^{n_4-n_1}\right) \\ \leqslant & 2^{n_1-1}\left(1 + 1 + 2^{-1} + 2^{-2}\right) = 2^{n_1-1}\left(2 + 2^{-1} + 2^{-2}\right) \\ < & 2^{n_1+1}. \end{aligned}$$

D'où

$$2^a < 2^{n_1+1} \Longrightarrow a < n_1 + 1 \Longrightarrow a \leqslant n_1.$$

Cette inégalité va nous aider à calculer certains paramètres.

En réécrivant l'équation (3.38), on obtient

$$\frac{\alpha^{n_1}}{\sqrt{5}} - 2^a = \frac{\beta^{n_1}}{\sqrt{5}} - (F_{n_2} + F_{n_3} + F_{n_4}).$$

En prenant en valeurs absolues l'équation ci-dessus, on obtient

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^a\right| \leqslant \left|\frac{\beta^{n_1}}{\sqrt{5}}\right| + (F_{n_2} + F_{n_3} + F_{n_4}) < \frac{|\beta|^{n_1}}{\sqrt{5}} + (\alpha^{n_2} + \alpha^{n_3} + \alpha^{n_4}),$$

et

$$\left|\frac{\alpha^{n_1}}{\sqrt{5}} - 2^a\right| < \frac{1}{2} + (\alpha^{n_2} + \alpha^{n_3} + \alpha^{n_4}) \quad \text{où nous avons utilisé} \quad F_n \leqslant \alpha^{n-1}.$$

En divisant les deux côtés de l'équation ci-dessus par $\alpha^{n_1}/\sqrt{5}$, on obtient

$$\begin{aligned}\left|1 - 2^a \cdot \alpha^{-n_1} \cdot \sqrt{5}\right| &< \frac{\sqrt{5}}{2\alpha^{n_1}} + \left(\alpha^{n_2-n_1} + \alpha^{n_3-n_1} + \alpha^{n_4-n_1}\right)\sqrt{5} \\ &< \frac{\sqrt{5}}{2\alpha^{n_1}} + \frac{\sqrt{5}}{\alpha^{n_1-n_2}} + \frac{\sqrt{5}}{\alpha^{n_1-n_3}} + \frac{\sqrt{5}}{\alpha^{n_1-n_4}}.\end{aligned}$$

Compte tenu de l'hypothèse $n_4 \leqslant n_3 \leqslant n_3 \leqslant n_2 \leqslant n_1$, on obtient

$$|\Lambda_1| = \left|1 - 2^a \cdot \alpha^{-n_1} \cdot \sqrt{5}\right| < \frac{9}{\alpha^{n_1-n_2}} \tag{3.39}$$

Appliquons le théorème de Matveev, avec les paramètres suivants $t := 3$ et

$$\gamma_1 := 2, \quad \gamma_2 := \alpha, \quad \gamma_3 := \sqrt{5}, \quad b_1 := a, \quad b_2 := -n, \quad \text{et} \quad b_3 := 1.$$

Puisque $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{K} := \mathbb{Q}(\sqrt{5})$, on peut prendre $D := 2$. Avant d'appliquer le théorème de Matveev, nous devons vérifier la dernière condition : le membre de gauche de l'équation (3.39) doit être différent de zéro. En effet, s'il était nul, on obtiendrait alors $2^a\sqrt{5} = \alpha^n$. En mettant au carré la relation précédente, on obtient $\alpha^{2n} = 5 \cdot 2^{2a} = 5 \cdot 4^a$. Cela implique que $\alpha^{2n} \in \mathbb{Z}$. Ce qui est impossible. D'où $\Lambda_1 \neq 0$. Les hauteurs logarithmiques de γ_1, γ_2 et γ_3 sont :

$h(\gamma_1) = \log 2 = 0.6931\ldots$, donc on peut choisir $A_1 := 1.4$.

$h(\gamma_2) = \dfrac{1}{2}\log\alpha = 0.2406\ldots$, donc on peut choisir $A_2 := 0.5$.

$h(\gamma_3) = \log\sqrt{5} = 0.8047\ldots$, il s'ensuit que l'on peut choisir $A_3 := 1.7$.

Puisque $a < n_1 + 1$, $B := \max\{|b_1|, |b_2|, |b_3|\} = n_1$. Le résultat de Matveev montre que

$$\left|1 - 2^a \cdot \alpha^{n_1} \cdot \sqrt{5}\right| > \exp\left(-c_1 \cdot (1 + \log n) \cdot 1.4 \cdot 0.5 \cdot 1.7\right), \tag{3.40}$$

où $c_1 := 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1 + \log 2) < 9.7 \times 10^{11}$.

En prenant log dans l'inégalité (3.39), on obtient

$$\log|\Lambda_1| < \log 9 - (n_1 - n_2)\log\alpha.$$

En prenant log dans l'inégalité (3.39), on obtient

$$\log|\Lambda_1| > 2.31 \times 10^{12} \log n_1.$$

En comparant les deux inégalités précédentes, on obtient

$$(n_1 - n_2)\log\alpha - \log 9 < 2.31 \times 10^{12} \log n_1,$$

où nous avons utilisé $1 + \log n_1 < 2\log n_1$. Ce qui est valide pour tout $n_1 \geqslant 3$. Ensuite nous avons

$$(n_1 - n_2)\log\alpha < 2.32 \times 10^{12} \log n_1. \tag{3.41}$$

Considérons maintenant une seconde forme linéaire de logarithmes. Réécrivons l'équation (3.38) comme suit

$$\frac{\alpha^{n_1}}{\sqrt{5}} + \frac{\alpha^{n_2}}{\sqrt{5}} - 2^a = \frac{\beta^{n_1}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}} - (F_{n_3} + F_{n_4}).$$

En prenant en valeurs absolues l'équation ci-dessus et le fait que $\beta = (1 - \sqrt{5})/2$, nous obtenons

$$\begin{aligned}\left|\frac{\alpha^{n_1}}{\sqrt{5}}\left(1 + \alpha^{n_2 - n_1}\right) - 2^a\right| \leqslant & \frac{|\beta|^{n_1} + |\beta|^{n_2}}{\sqrt{5}} + F_{n_3} + F_{n_4} \\ < & \frac{1}{3} + \alpha^{n_3} + \alpha^{n_4} \quad \text{pour tout} \quad n_1 \geqslant 5 \quad \text{et} \quad n_2 \geqslant 5.\end{aligned}$$

En divisant les deux membres de l'inégalité ci-dessus par $\frac{\alpha^{n_1}}{\sqrt{5}}\left(1 + \alpha^{n_2 - n_1}\right)$, on obtient

$$|\Lambda_2| = \left|1 - 2^a \cdot \alpha^{n_1} \cdot \sqrt{5}\left(1 + \alpha^{n_2 - n_1}\right)^{-1}\right| < \frac{6}{\alpha^{n_2 - n_1}}. \tag{3.42}$$

Appliquons le théorème de Matveev une seconde fois avec les données suivantes

$$t := 3, \quad \gamma_1 := 2, \quad \gamma_2 := \alpha, \quad \gamma_3 := \sqrt{5}\left(1+\alpha^{n_2-n_1}\right)^{-1},$$

$$b_1 := a, \quad b_2 := -n_1, \quad \text{et} \quad b_3 := 1.$$

Puisque $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{K} := \mathbb{Q}(\sqrt{5})$, on peut prendre $D := 2$. Le terme gauche de l'équation (3.42) n'est pas nul, sinon, nous obtiendrions la relation

$$2^a\sqrt{5} = \alpha^{n_1} + \alpha^{n_2}. \tag{3.43}$$

En prenant le conjugué de l'équation (3.43) dans le corps $\mathbb{Q}(\sqrt{5})$, on obtient

$$-2^a\sqrt{5} = \beta^{n_1} + \beta^{n_2}. \tag{3.44}$$

En combinant les équations (3.43) et (3.44), on obtient

$$\alpha^{n_1} < \alpha^{n_1} + \alpha^{n_2} = |\beta^{n_1} + \beta^{n_2}| \leqslant |\beta|^{n_1} + |\beta|^{n_2} < 1$$

ce qui est impossible pour $n_1 > 350$. D'où $\Lambda_2 \neq 0$. On sait que $h(\gamma_1) = \log 2$ et $h(\gamma_2) = \frac{1}{2}\log\alpha$. Estimons maintenant $h(\gamma_3)$ en observant d'abord que

$$\gamma_3 = \frac{\sqrt{5}}{1+\alpha^{n_2-n_1}} < \sqrt{5} \quad \text{and} \quad \gamma_3^{-1} = \frac{1+\alpha^{n_2-n_1}}{\sqrt{5}} < \frac{2}{\sqrt{5}},$$

de sorte que $|\log\gamma_3| < 1$. En utilisant les propriétés de hauteur logarithmique énoncées dans la Proposition 3.2.2, nous avons

$$h(\gamma_3) \leqslant \log\sqrt{5} + |n_2 - n_1|\left(\frac{\log\alpha}{2}\right) + \log 2 = \log(2\sqrt{5}) + (n_1 - n_2)\left(\frac{\log\alpha}{2}\right).$$

Par conséquent, nous pouvons prendre $A_3 := 3 + (n_1 - n_2)\log\alpha > \max\{2h(\gamma_3), |\log\gamma_3|, 0.16\}$.

Le théorème de Matveev implique que

$$\exp\left(-c_2(1+\log n_1)\cdot 1.4\cdot 0.5\cdot(3+(n_1-n_2)\log\alpha)\right)$$

où $c_2 := 1.4\cdot 30^6\cdot 3^{4.5}\cdot 2^2\cdot(1+\log 2) < 9.7\times 10^{11}$.

Vue que $(1+\log n_1) < 2\log n_1$ est vérifiée pour $n_1 \geqslant 3$, de l'équation (3.42), nous avons

$$(n_1 - n_3)\log\alpha - \log 6 < 1.4 \times 10^{12}\log n_1(3 + (n_1 - n_2)\log\alpha). \tag{3.45}$$

En mettant la relation (3.41) dans le terme de droite de l'équation (3.45), on obtient

$$(n_1 - n_3)\log\alpha < 3.29 \times 10^{24}\log^2 n_1. \tag{3.46}$$

Considérons une troisième forme linéaire de logarithmes. Pour ce faire, réécrivons à nouveau l'équation (3.38) comme suit

$$\frac{\alpha^{n_1} + \alpha^{n_2} + \alpha^{n_3}}{\sqrt{5}} - 2^a = \frac{\beta^{n_1} + \beta^{n_2} + \beta^{n_3}}{\sqrt{5}} - F_{n_4}.$$

En prenant en valeurs absolues l'équation ci-dessus, on obtient

$$\begin{aligned}\left|\frac{\alpha^{n_1}}{\sqrt{5}}\left(1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1}\right) - 2^a\right| &\leqslant \frac{|\beta|^{n_1} + |\beta|^{n_2} + |\beta|^{n_3}}{\sqrt{5}} + F_{n_4} \\ &< \frac{3}{4} + \alpha^{n_4} \quad \text{pour tout} \quad n_1 > 350, \quad \text{et} \quad n_2, n_3, n_4 \geqslant 1.\end{aligned}$$

Ainsi nous avons

$$|\Lambda_3| = \left|1 - 2^a \cdot \alpha^{-n_1} \cdot \sqrt{5}\left(1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1}\right)^{-1}\right| < \frac{3}{\alpha^{n_1-n_4}}. \tag{3.47}$$

Dans une troisième application du théorème de Matveev, on peut prendre des paramètres

$$t := 3, \quad \gamma_1 := 2, \quad \gamma_2 := \alpha, \quad \gamma_3 := \sqrt{5}\left(1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1}\right)^{-1},$$

$$b_1 := a, \quad b_2 := -n, \quad \text{et}, \quad b_3 := 1.$$

Puisque $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{K} := \mathbb{Q}(\sqrt{5})$, nous pouvons prendre $D := 2$. Le côté gauche de l'équation (3.47) n'est pas nul. La preuve se fait par contradiction. Supposons le contraire. Alors

$$2^a\sqrt{5} = \alpha^{n_1} + \alpha^{n_2} + \alpha^{n_3}.$$

En prenant le conjugué dans le corps $\mathbb{Q}(\sqrt{5})$, on obtient

$$-2^a\sqrt{5} = \beta^{n_1} + \beta^{n_2} + \beta^{n_3},$$

qui conduit à

$$\alpha^{n_1} < \alpha^{n_1} + \alpha^{n_2} + \alpha^{n_3} = |\beta^{n_1} + \beta^{n_2} + \beta^{n_3}| \leqslant |\beta|^{n_1} + |\beta|^{n_2} + |\beta|^{n_3} < 1$$

et conduit à une contradiction puisque $n_1 > 350$. D'où $\Lambda_3 \neq 0$. Comme précédemment, nous pouvons prendre $A_1 := 1.4$, $A_2 := 0.5$ et $B := n_1$. Nous pouvons également voir que

$$\gamma_3 = \frac{\sqrt{5}}{1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1}} < \sqrt{5} \quad \text{et} \quad \gamma_3^{-1} = \frac{1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1}}{\sqrt{5}} < \frac{3}{\sqrt{5}},$$

ainsi $|\log \gamma_3| < 1$. En appliquant les propriétés sur la hauteur logarithmique, nous estimons $h(\gamma_3)$. D'où

$$\begin{aligned} h(\gamma_3) &\leqslant \log\sqrt{5} + |n_2 - n_1|\left(\frac{\log\alpha}{2}\right) + |n_3 - n_1|\left(\frac{\log\alpha}{2}\right) + \log 3 \\ &= \log(3\sqrt{5}) + (n_1 - n_2)\left(\frac{\log\alpha}{2}\right) + (n_1 - n_3)\left(\frac{\log\alpha}{2}\right); \end{aligned}$$

donc on peut prendre

$$A_3 := 4 + (n_1 - n_2)\log\alpha + (n_1 - n_3)\log\alpha > \max\{2h(\gamma_3), |\log\gamma_3|, 0.16\}.$$

Une borne inférieure du terme de gauche de l'équation (3.47) est

$$\exp(-c_3 \cdot (1 + \log n_1) \cdot 1.4 \cdot 0.5 \cdot (4 + (n_1 - n_2)\log\alpha + (n_1 - n_3)\log\alpha))$$

où $c_3 = 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1 + \log 2) < 9.7 \times 10^{11}$.

A partir de l'inégalité (3.47), on a

$$(n_1 - n_4)\log\alpha < 1.4 \times 10^{12} \log n_1 \cdot (4 + (n_1 - n_2)\log\alpha + (n_1 - n_3)\log\alpha). \tag{3.48}$$

En combinant les inégalités (3.41) et (3.46) dans les termes de droite de l'équation (3.48) et en effectuant les calculs respectifs, nous obtenons

$$(n_1 - n_4)\log\alpha < 9.3 \times \log^3 n_1. \tag{3.49}$$

Considérons maintenant une quatrième et dernière forme linéaire de logarithmes. En réécrivant l'équation (3.38) encore une fois et en séparant les grands termes et les petits termes, on obtient

$$\frac{\alpha^{n_1} + \alpha^{n_2} + \alpha^{n_3} + \alpha^{n_4}}{\sqrt{5}} - 2^a = \frac{\beta^{n_1} + \beta^{n_2} + \beta^{n_3} + \beta^{n_4}}{\sqrt{5}}.$$

En prenant en valeurs absolues l'équation suivante, on obtient

$$\begin{aligned}\left|\frac{\alpha^{n_1}}{\sqrt{5}}\left(1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1} + \alpha^{n_4-n_1}\right) - 2^a\right| \leqslant & \frac{|\beta|^{n_1} + |\beta|^{n_2} + |\beta|^{n_3} + |\beta|^{n_4}}{\sqrt{5}} \\ < & \frac{4}{5} \quad \text{pour tout} \quad n_1 > 350, \quad \text{et} \quad n_2, n_3, n_4 \geqslant 1.\end{aligned}$$

En divisant les deux membres de la relation ci-dessus par le premier terme du membre de droite de l'équation précédente, nous obtenons

$$|\Lambda_4| = \left|1 - 2^a \cdot \alpha^{-n_1} \cdot \sqrt{5}\left(1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1} + \alpha^{n_4-n_1}\right)^{-1}\right| < \frac{2}{\alpha^{n_1}}. \tag{3.50}$$

Dans la dernière application du théorème de Matveev, on a les paramètres suivants

$$\gamma_1 := 2, \quad \gamma_2 := \alpha, \quad \gamma_3 := \sqrt{5}\left(1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1} + \alpha^{n_4-n_1}\right)^{-1},$$

et on peut aussi prendre $b_1 := a, \quad b_2 := -n$ et $b_3 := 1$. Vu que $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{K} := \mathbb{Q}(\sqrt{5})$, on peut prendre $D := 2$. Le terme gauche de l'équation (3.50) est différent de zéro. La preuve se fait par contradiction. Supposons le contraire. Alors

$$2^a\sqrt{5} = \alpha^{n_1} + \alpha^{n_2} + \alpha^{n_3} + \alpha^{n_4}.$$

Conjuguer la relation ci-dessus sur le corps $\mathbb{Q}(\sqrt{5})$, on obtient

$$-2^a\sqrt{5} = \beta^{n_1} + \beta^{n_2} + \beta^{n_3} + \beta^{n_4}.$$

En combinant les deux équations ci-dessus, on obtient

$$\alpha^{n_1} < \alpha^{n_1} + \alpha^{n_2} + \alpha^{n_3} + \alpha^{n_4} = |\beta^{n_1} + \beta^{n_2} + \beta^{n_3} + \beta^{n_4}| \leqslant |\beta|^{n_1} + |\beta|^{n_2} + |\beta|^{n_3} + |\beta|^{n_4} < 1,$$

et conduit à la contradiction puisque $n_1 > 350$.

Comme précédemment, ici, nous pouvons prendre $A_1 := 1.4$, $A_2 := 0.5$ et $B := n_1$. Estimons $h(\gamma_3)$. On peut voir que,

$$\gamma_3 = \frac{\sqrt{5}}{1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1} + \alpha^{n_4-n_1}} < \sqrt{5}$$

$$\text{and} \quad \gamma_3^{-1} = \frac{1 + \alpha^{n_2-n_1} + \alpha^{n_3-n_1} + \alpha^{n_4-n_1}}{\sqrt{5}} < \frac{4}{\sqrt{5}}.$$

D'où$|\log \gamma_3| < 1$. Alors

$$\begin{aligned} h(\gamma_3) &\leqslant \log(4\sqrt{5}) + |n_2 - n_1| \left(\frac{\log \alpha}{2}\right) + |n_3 - n_1| \left(\frac{\log \alpha}{2}\right) + |n_4 - n_1| \left(\frac{\log \alpha}{2}\right) \\ &= \log(4\sqrt{5}) + (n_1 - n_2) \left(\frac{\log \alpha}{2}\right) + (n_1 - n_3) \left(\frac{\log \alpha}{2}\right) + (n_1 - n_4) \left(\frac{\log \alpha}{2}\right); \end{aligned}$$

donc on peut prendre

$$A_3 := 5 + (n_1 - n_2) \log \alpha + (n_1 - n_3) \log \alpha + (n_1 - n_4) \log \alpha.$$

Alors une borne inférieure du terme gauche de l'inégalité (3.50) est

$$\exp(-c_4 \cdot (1 + \log n_1) \cdot 1.4 \cdot 0.5 \cdot (5 + (n_1 - n_2) \log \alpha + (n_1 - n_3) \log \alpha + (n_1 - n_4) \log \alpha)),$$

où $c_4 = 1.4 \cdot 30^6 \cdot 3^{4.5} \cdot 2^2 \cdot (1 + \log 2) < 9.7 \times 10^{11}$.

Ainsi, l'inégalité (3.50) donne

$$n_1 \log \alpha < 1.4 \times 10^{12} \log n_1 \cdot (5 + (n_1 - n_2) \log \alpha + (n_1 - n_3) \log \alpha + (n_1 - n_4) \log \alpha). \quad (3.51)$$

En utilisant maintenant les inégalités (3.41), (3.46) et (3.49) dans les termes de droite de l'inégalité (3.51) et en effectuant les calculs respectifs, nous trouvons que

$$n_1 \log \alpha < 40.32 \times 10^{48} \log^4 n_1.$$

A l'aide de *Mathematica*, on obtient de l'inégalité précédente

$$n_1 < 2.8 \times 10^{58}.$$

Nous résumons ce que nous avons prouvé.

Lemme 3.5.1.

Si (n_1, n_2, n_3, n_4, a) est une solution positive de l'équation (3.38) avec $n_1 \geqslant n_2 \geqslant n_3 \geqslant n_4$, alors

$$a \leqslant n_1 < 2.8 \times 10^{58}.$$

3.5.3 Réduction

Le but de cette section est de réduire la borne supérieure de n_1 à une taille qui peut être gérée. Pour ce faire, nous utiliserons quatre fois le Lemme 3.2.4. Considérons

$$z_1 := a \log 2 - n_1 \log \alpha + \log \sqrt{5}. \tag{3.52}$$

De l'équation (3.52), (3.39) peut être écrit comme suit

$$|1 - e^{z_1}| < \frac{9}{\alpha^{n_1 - n_2}}. \tag{3.53}$$

En associant l'équation (3.38) et la formule de Binet pour la suite de Fibonacci, on a

$$\frac{\alpha^{n_1}}{\sqrt{5}} = F_{n_1} + \frac{\beta^{n_1}}{\sqrt{5}} < F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a,$$

d'où

$$\frac{\alpha^{n_1}}{\sqrt{5}} < 2^a,$$

ce qui conduit à $z_1 > 0$. Ce résultat avec l'inégalité (3.53), donne

$$0 < z_1 < e^{z_1} - 1 < \frac{9}{\alpha^{n_1 - n_2}}.$$

En remplaçant l'équation (3.52) dans l'inégalité et en divisant les deux côtés de l'inégalité résultante par $\log \alpha$, on obtient

$$0 < a\left(\frac{\log 2}{\log \alpha}\right) - n + \left(\frac{\log \sqrt{5}}{\log \alpha}\right) < \frac{9}{\log \alpha} \cdot \alpha^{n_1 - n_2} < 19 \cdot \alpha^{n_1 - n_2}. \tag{3.54}$$

Nous mettons

$$\tau := \frac{\log 2}{\log \alpha}, \quad \mu := \frac{\log \sqrt{5}}{\log \alpha}, \quad A := 19, \quad \text{et} \quad B := \alpha.$$

τ est un nombre irrationnel. On pose aussi $M := 2.8 \times 10^{58}$, qui est une majoration de a par le Lemme 3.2.4 appliqué à l'inégalité, que

$$n_1 - n_2 < \frac{\log(Aq/\varepsilon)}{\log B},$$

où $q > 6M$ est un dénominateur d'un convergent de la fraction continue de τ tel que $\varepsilon := \|\mu q\| - M\|\tau q\| > 0$. Un calcul avec *SageMath* a révélé que si (n_1, n_2, n_3, n_4, a) est une solution possible de l'équation (3.38), alors

$$n_1 - n_2 \in [0, 314].$$

Considérons maintenant une seconde fonction, dérivée de (3.42) afin de trouver une borne supérieure améliorée sur $n_1 - n_2$.

Posons

$$z_2 := a \log 2 - n_1 \log \alpha + \log \Upsilon_1(n_1 - n_2)$$

où Υ est la fonction donnée par la formule $\Upsilon(t) := \sqrt{5}\left(1 + \alpha^{-t}\right)^{-1}$. De (3.42), nous avons

$$|1 - e^{z_2}| < \frac{6}{\alpha^{n_1 - n_3}}. \tag{3.55}$$

En utilisant (3.38) et la formule de Binet pour la suite de Fibonacci, nous avons

$$\frac{\alpha^{n_1}}{\sqrt{5}} + \frac{\alpha^{n_2}}{\sqrt{5}} = F_{n_1} + F_{n_2} + \frac{\beta^{n_1}}{\sqrt{5}} + \frac{\beta^{n_2}}{\sqrt{5}} < F_{n_1} + F_{n_2} + 1 \leqslant F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a.$$

Donc $1 < 2^a \sqrt{5} \alpha^{-n_1} \left(1 + \alpha^{n_2 - n_1}\right)^{-1}$ et donc $z_2 > 0$. Ceci avec (3.55) donne

$$0 < z_2 \leqslant e^{z_2} - 1 < \frac{6}{\alpha^{n_1 - n_3}}.$$

En mettant l'expression de z_2 dans l'inégalité ci-dessus et en argumentant comme dans (3.54), nous obtenons

$$0 < a\left(\frac{\log 2}{\log \alpha}\right) - n_1 + \frac{\log \Upsilon_1(n_1 - n_2)}{\log \alpha} < 13 \cdot \alpha^{-(n_1 - n_3)}. \tag{3.56}$$

Comme précédemment, on reprend $M := 2.8 \times 10^{58}$ qui est la borne supérieure de a, et, comme expliqué précédemment, on applique le Lemme 3.2.4 à l'inégalité (3.56) pour tous les choix $n_1 - n_2 \in [0, 314]$ sauf lorsque $n_1 - n_2 = 2, 6$. A l'aide de *SageMath*, on trouve que si (n_1, n_2, n_3, n_4, a) est une solution possible de l'équation (3.38) avec $n_1 - n_2 \neq 2$ et $n_1 - n_2 \neq 6$, alors $n_1 - n_3 \in [0, 314]$.

Étude des cas $n_1 - n_2 \in \{2, 6\}$. Pour ces cas, lorsqu'on applique le Lemme 3.2.4 à l'expression (3.56), le paramètre correspondant μ apparaissant dans le lemme 3.2.4 est

$$\frac{\log Y_1(t)}{\log \alpha} = \begin{cases} 1 & \text{si} \quad t = 2; \\ 3 - \dfrac{\log 2}{\log \alpha} & \text{si} \quad t = 6. \end{cases}$$

Dans les deux cas, les paramètres τ et μ sont linéairement dépendants, ce qui fait que la valeur correspondante de ε du Lemme 3.2.4 est toujours négative et donc la méthode de réduction n'est pas utile pour réduire la borne sur n dans ces cas. Pour cela, nous devons traiter ces cas différemment.

Cependant, nous pouvons voir que si $t = 2$ et 6, alors l'inégalité résultante de (3.56) a la forme $0 < |x\tau - y| < 13 \cdot \alpha^{-(n_1 - n_3)}$ avec τ étant un nombre irrationnel et $x, y \in \mathbb{Z}$. Ensuite, en utilisant les propriétés connues des convergentes des fractions continues pour obtenir une borne inférieure non triviale pour $|x\tau - y|$. Voyons comment faire.

Pour $n_1 - n_2 = 2$, de (3.56), on obtient que

$$0 < a\tau - (n_1 - 1) < 13 \cdot \alpha^{-(n_1 - n_3)}, \quad \text{où} \quad \tau = \frac{\log 2}{\log \alpha}. \tag{3.57}$$

Soit $[a_1, a_2, a_3, a_4, \ldots] = [1, 2, 3, 1, \ldots]$ soit la fraction continue de τ, et notons p_k/q_k le $k^{\text{ème}}$ convergent. Par le Lemme 3.2.3, on sait que $a < 2.8 \times 10^{58}$. Une inspection dans *SageMath* révèle que

$$120747114404749145151211009265773033280880919910535418568 5 = q_{113} < 2.8 \times 10^{58} <$$

$$q_{114} = 283510969291951871695176865758418993091291968591709388216 67.$$

De plus, $a_M := \max\{a_i : i = 0, 1, \ldots, 114\} = 134$. Donc, d'après les propriétés des fractions continues, on obtient que

$$|a\tau - (n_1 - 1)| > \frac{1}{(a_M + 2)a}. \tag{3.58}$$

En comparant les inégalités (3.57) et (3.58), nous obtenons

$$\alpha^{n_1-n_3} < 13 \cdot (134+2)a.$$

En prenant log des deux côtés de l'équation ci-dessus et en divisant le résultat obtenu par $\log \alpha$, on obtient

$$n_1 - n_3 < 296.$$

Afin d'éviter les répétitions, nous omettons librement les détails pour le cas $n_1 - n_2 = 6$. Ici, nous obtenons $n_1 - n_3 < 314$.

Ceci termine l'analyse des deux cas particuliers $n_1 - n_2 = 2$ et $n_1 - n_2 = 6$. Par conséquent $n_1 - n_3 \leqslant 314$ est toujours valable.

Utilisons maintenant l'inégalité (3.47) pour trouver une borne supérieure améliorée sur $n_1 - n_4$. Posons

$$z_3 := a \log 2 - n_1 \log \alpha + \log \mathrm{Y}_2(n_1 - n_2, n_1 - n_3),$$

où Y_2 est la fonction donnée par la formule $\mathrm{Y}_2(t,s) := \sqrt{5}\left(1 + \alpha^{-t} + \alpha^{-s}\right)^{-1}$. De l'inégalité (3.47), nous avons

$$|1 - e^{z_3}| < \frac{3}{\alpha^{n_1-n_4}}. \tag{3.59}$$

Notons que , $z_3 \neq 0$; ainsi, deux cas se présentent : $z_3 > 0$ et $z_3 < 0$.

Si $z_3 > 0$, alors

$$0 < z_3 \leqslant e^{z_3} - 1 < \frac{3}{\alpha^{n_1-n_4}}.$$

Supposons maintenant $z_3 < 0$. Il est facile de vérifier que $3/\alpha^{n_1-n_4} < 1/2$ pour tout $n_1 > 350$ et $n_4 \geqslant 2$. De l'inégalité (3.59), nous savons que

$$|1 - e^{z_3}| < 1/2 \quad \text{alors} \quad e^{|z_3|} < 2.$$

Puisque $z_3 < 0$, nous avons :

$$0 < |z_3| \leqslant e^{|z_3|} - 1 = e^{|z_3|}\left|e^{|z_3|} - 1\right| < \frac{6}{\alpha^{n_1-n_4}}$$

qui donnent

$$0 < |z_3| < \frac{6}{\alpha^{n_1-n_4}}$$

est valable pour $z_3 < 0$, $z_3 > 0$ et pour tout pour tout $n_1 > 350$, et $n_4 \geqslant 2$. En remplaçant l'expression de z_3 dans l'inégalité ci-dessus et en argumentant à nouveau comme avant, nous concluons que

$$0 < \left| a\left(\frac{\log 2}{\log \alpha}\right) - n_1 + \frac{\log Y_2(n_1 - n_2, n_1 - n_3)}{\log \alpha} \right| < 13 \cdot \alpha^{-(n_1 - n_4)}. \tag{3.60}$$

Ici, on prend aussi $M := 2.8 \times 10^{58}$ et on applique le lemme 3.2.4 à l'inégalité (3.60) pour tous les choix $n_1 - n_2 \in \{0, 314\}$ et $n_1 - n_3 \in \{0, 314\}$ sauf quand

$$(n_1 - n_2, n_1 - n_3) \in \{(0,3), (1,1), (1,5), (3,0), (3,4), (4,3), (5,1), (7,8), (8,7)\}.$$

En effet, à l'aide de *SageMath* nous trouvons que si (n_1, n_2, n_3, n_4, a) est une solution possible de l'équation (3.38) en excluant les cas présentés précédemment. Puis $n_1 - n_4 \leqslant 314$.

CAS SPÉCIAUX : Nous traitons les cas où

$$(n_1 - n_2, n_1 - n_3) \in \{(1,1), (3,0), (4,3), (5,1), (8,7)\}.$$

Il est facile de vérifier que

$$\frac{\log Y_2(t,s)}{\log \alpha} = \begin{cases} 0, & \text{si} \quad (t,s) = (1,1); \\ 0, & \text{si} \quad (t,s) = (3,0); \\ 1, & \text{si} \quad (t,s) = (4,3); \\ 2 - \dfrac{\log 2}{\log \alpha}, & \text{si} \quad (t,s) = (5,1); \\ 3 - \dfrac{\log 2}{\log \alpha}, & \text{si} \quad (t,s) = (8,7). \end{cases}$$

Comme nous l'avons expliqué précédemment, lorsque nous appliquons le lemme 3.2.4 à l'expression (3.60), les paramètres τ et μ sont linéairement dépendants, donc la valeur correspondante de ε du lemme 3.2.4 est toujours négative dans tous les cas. Pour cette raison, nous traiterons ces cas différemment.

Ici, il faut résoudre les équations

$$F_{n_2+1} + 2F_{n_2} + F_{n_4} = 2^a, \quad 2F_{n_2+3} + F_{n_2} + F_{n_4} = 2^a, \quad F_{n_2+4} + F_{n_2} + F_{n_2+1} + F_{n_4} = 2^a,$$

$$F_{n_2+5} + F_{n_2} + F_{n_2+4} + F_{n_4} = 2^a, \quad \text{et} \quad F_{n_2+8} + F_{n_2} + F_{n_2+1} + F_{n_4} = 2^a \tag{3.61}$$

d'inconnus, les entiers positifs n_2, n_4 et a. Pour ce faire, rappelons la relation bien connue suivante entre les nombres de Fibonacci et de Lucas :

$$L_k = F_{k-1} + F_{k+1} \quad \text{pour tout} \quad k \geqslant 1. \tag{3.62}$$

Des équations (3.62) et (3.61), nous avons les identités suivantes

$$\begin{gathered}
F_{n_2+1} + 2F_{n_2} + F_{n_4} = F_{n_2+2} + F_{n_2} + F_{n_4} = F_{k+2} + F_k + F_m, \\
2F_{n_2+3} + F_{n_2} + F_{n_4} = F_{n_2+2} + F_{n_2+4} + F_{n_4} = F_{k+2} + F_{k+4} + F_m, \\
F_{n_2+4} + F_{n_2} + F_{n_2+1} + F_{n_4} = F_{n_2+2} + F_{n_2+4} + F_{n_4} = F_{k+2} + F_{k+4} + F_m, \\
F_{n_2+5} + F_{n_2} + F_{n_2+4} + F_{n_4} = 2F_{n_2+2} + 2F_{n_2+4} + F_{n_4} = 2F_{k+2} + 2F_{k+4} + F_m, \\
\text{et} \quad F_{n_2+8} + F_{n_2} + F_{n_2+1} + F_{n_4} = 2F_{n_2+6} + 2F_{n_2+4} + F_{n_4} = 2F_{k+6} + 2F_{k+4} + F_m,
\end{gathered} \tag{3.63}$$

est valide pour tout $k, m \geqslant 0$.

Les équations de (3.61) sont transformés en équations

$$L_{k+1} + F_m = 2^a, \quad L_{k+3} + F_m = 2^a, \quad 2L_{k+3} + F_m = 2^a, \quad 2L_{k+5} + F_m = 2^a, \tag{3.64}$$

à résoudre, d'inconnus, les entiers positifs k, m et a.

Une recherche rapide dans *SageMath* et une résolution analytique conduit à :

$$(k, m, a) \in \{(4, 5, 4), (4, 8, 5)\} \quad \text{pour} \quad L_{k+1} + F_m = 2^a,$$

$$(k, m, a) \in \{(2, 5, 4), (2, 8, 5), (4, 4, 5)\} \quad \text{pour} \quad L_{k+3} + F_m = 2^a,$$

$$(k, m, a) = (5, 9, 7) \quad \text{pour} \quad 2L_{k+3} + F_m = 2^a,$$

$$(k, m, a) = (3, 9, 7) \quad \text{pour} \quad 2L_{k+5} + F_m = 2^a.$$

Une résolution et une analyse complètes donnent des solutions déjà listées dans le Théorème

3.5.1. Ceci termine l'analyse des cas particuliers.

Enfin, utilisons (3.50) pour trouver une borne supérieure améliorée sur n_1. Posons

$$z_4 := a\log 2 - n_1\log\alpha + \log \mathrm{Y}_3(n_1-n_2, n_1-n_3, n_1-n_4),$$

où Y_3 est la fonction donnée par la formule

$$\mathrm{Y}_3(t,u,v) := \sqrt{5}\left(1+\alpha^{-t}+\alpha^{-u}+\alpha^{-v}\right)^{-1}$$

avec $t = n_1 - n_2, u = n_1 - n_3$ et $v = n_1 - n_4$. De (3.50), nous avons

$$|1 - e^{z_3}| < \frac{2}{\alpha^{n_1}}. \tag{3.65}$$

Puisque $z_3 \neq 0$, comme précédemment, deux cas se présentent : $z_4 < 0$ et $z_4 > 0$.

Si $z_4 > 0$, alors

$$0 < z_4 \leqslant e^{z_4} - 1 < \frac{2}{\alpha^{n_1}}.$$

Supposons maintenant que $z_4 < 0$. Nous avons $2/\alpha^{n_1} < 1/2$ pour tous les $n_1 > 350$. Ensuite, à partir de (3.65), nous avons

$$|1 - e^{z_4}| < \frac{1}{2}$$

et donc $e^{|z_3|} < 2$.

Puisque $z_3 < 0$, on a :

$$0 < |z_3| \leqslant e^{|z_3|} - 1 = e^{|z_3|}\left|e^{|z_3|} - 1\right| < \frac{4}{\alpha^{n_1}}$$

qui donne

$$0 < |z_3| < \frac{4}{\alpha^{n_1}}$$

pour les deux cas ($z_3 < 0$ et $z_3 > 0$) et est valable pour tous les $n_1 > 350$.

En remplaçant l'expression de z_3 dans l'inégalité ci-dessus et en argumentant à nouveau comme avant, nous concluons que

$$0 < \left| a\left(\frac{\log 2}{\log\alpha}\right) - n_1 + \frac{\log \mathrm{Y}_3(n_1-n_2, n_1-n_3, n_1-n_4)}{\log\alpha}\right| < 9\cdot\alpha^{-n_1}. \tag{3.66}$$

Ici, on prend aussi $M := 2.8 \times 10^{58}$ et on applique le lemme 3.2.4 une dernière fois dans l'inégalité (3.66) pour tous les choix $n_1 - n_2 \in \{0, 314\}$, $n_1 - n_3 \in \{0, 314\}$ et $n_1 - n_4 \in \{0, 314\}$ avec (n_1, n_2, n_3, n_4, a) une possible solution de l'équation (3.38), et en omettant l'étude des cas particuliers (car cela donne une solution présentée dans le théorème 3.5.1), on obtient :

$$n_1 < 320.$$

Ceci est faux car notre hypothèse dit que $n_1 > 350$.

Ceci termine la preuve de notre théorème principal.

□

Remarque 3.5.1.

Notez que les calculs pour ce dernier cas ont pris 2 *heures sur un ordinateur ASUS Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz.*

3.6 Commentaires

Dans cet article, nous avons trouvé tous les cas dans lesquels une puissance de deux peut être exprimée comme une somme de quatre nombres de Fibonacci. Compte tenu des résultats obtenus, nous pouvons faire la conjecture suivante.

Conjecture 3.6.1.

Considérons l'équation Diophantienne

$$F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = p^a, p \geqslant 2, a \geqslant 2 \tag{3.67}$$

où n_1, n_2, n_3, n_4, a sont entiers positifs avec $n_1 \geqslant n_2 \geqslant n_3 \geqslant n_4$ et p premier, alors $p = 2, 3, 5, 7$.

Dans la section suivante, nous allons voir comment la méthode mathématique des équations Diophantiennes s'applique en physique et en chimie.

3.7 Méthode mathématique des équations Diophantiennes : applications en chimie et physique

Cette section est une version modifiée d'un article intitulé *Linear forms in Logarithms and the mathematical method of Diophantine equations : Applications in chemistry and physics*, publié dans **Journal of Mathematical Chemistry**, Volume 59, (2021), Pages $2009-2020$.

3.7.1 La méthode mathématique des équations Diophantiennes

Dans cette section, nous discuterons des applications de la méthode mathématique des équations Diophantiennes en chimie et en physique. En chimie, cette méthode est appliquée dans l'équilibrage des équations chimiques et dans la détermination de la formule moléculaire d'un composé. En physique, elle est appliquée dans la résolution de la troisième loi de Kepler.

3.7.2 La méthode mathématique des équations Diophantiennes en chimie

Tout d'abord, il y a certaines conditions auxquelles un problème doit satisfaire pour être abordable par cette méthode. Ces applications suggèrent que l'équation Diophantienne peut s'avérer utile pour attaquer d'autres problèmes de chimie. Supposons que l'on ait une équation en deux ou plusieurs inconnues ayant chacune des coefficients entiers et élevées à une puissance intégrale positive. On souhaite alors trouver juste des solutions intégrales à l'équation. De plus, les inconnues intégrales devraient rendre chaque terme entier ; en fait, il ne devrait alors y avoir aucun nombre décimal dans l'équation. L'équation de la forme $a_1x_1 + a_2x_2 + ... + a_nx_n = c$, où $a_1, a_2, ..., a_n, c$ sont des entiers est appelé équation Diophantienne linéaire ou équation Diophantienne du premier ordre. Dans cette section, toutes les équations sont linéaires. Le résultat de cette sous-section est dû à Roger Crocker, 1968.

3.7.2.1 Équilibrage d'équations chimiques

Étant donné l'équation chimique

$$xA_{a_1}B_{b_1}C_{c_1}\cdots + yA_{a_2}B_{b_2}C_{c_2}\cdots + \cdots \longrightarrow x'A_{a'_1}B_{b'_1}C_{c'_1}\cdots + y'A_{a'_2}B_{b'_2}C_{c'_2}\cdots + \cdots \quad (3.68)$$

où $a_1, b_1, c_1, \cdots, a'_1, b'_1, c'_1, \cdots$ sont nombres entiers positifs ou nuls, et où $x, y, \cdots, x', y', \cdots$ sont les coefficients inconnus des réactifs et des produits. Puis

$$\begin{aligned} xa_1 + ya_2 + \cdots &= x'a'_1 + y'a'_2 + \cdots \\ xb_1 + yb_2 + \cdots &= x'b'_1 + y'b'_2 + \cdots \\ xc_1 + yc_2 + \cdots &= x'c'_1 + y'c'_2 + \cdots \end{aligned} \tag{3.69}$$

C'est-à-dire qu'il y a une équation de chaque élément séparé $(A, B, C, \cdots)$ dans la réaction, exprimant la conservation du nombre d'atomes de cet élément. Chacune de ces équations est une équation Diophantienne car $x, y, \cdots, x', y', \cdots, a_1, a_2, \cdots, b_1, b_2, \cdots, \cdots$ sont tous entiers. Soit n' et n respectivement le nombre de termes et le nombre d'éléments. Si $n' > n$, on a un système de n équations Diophantiennes en n' inconnues. Ainsi après élimination des inconnues, on obtient une seule équation Diophantienne linéaire en $n' - n + 1$ inconnues, qui peut être résolue facilement par des règles simples. La situation $n' > n$ se produit extrêmement souvent, en particulier lorsque $n' - n = 1$, un cas dans lequel l'équation Diophantienne résultante peut être résolue immédiatement. $n' - n = 2$ est un cas dans lequel l'équation Diophantienne résultante peut être résolue facilement. Si $n' = n$, le système est dit complètement déterminé et aucune équation Diophantienne résultante ne se produit après élimination des inconnues. Or, si $n' < n$, le système est dit surdéterminé. Un système d'équations surdéterminés est un système avec plus d'équations que d'inconnues. Dans ce cas, les solutions supplémentaires sont non physiques (elles ne correspondent pas au problème étudié). Un système physique correctement analysé doit avoir un critère approprié pour éliminer les solutions non physiques.

En général, si deux ensembles de valeurs indépendantes ou plus satisfont (3.69), alors ils équilibrent tous l'équation (3.68) et, cette équation peut être équilibrée de plusieurs manières indépendantes.

Exemple 3.7.1.

$$xKMn0_4 + yH_2SO_4 + zH_2O_2 \longrightarrow x'K_2SO_4 + y'MnSO_4 + z'H_2O + w'O_2 \tag{3.70}$$

$\Longrightarrow$

$$\begin{aligned} 4x + 4y + 2z &= 4x' + 4y' + z' + 2w' \quad \text{pour} \quad O \\ x &= y' \quad \text{pour} \quad Mn \\ x &= 2x' \quad \text{pour} \quad K \\ y &= x' + y' \quad \text{pour} \quad S \\ 2y + 2z &= 2z' \quad \text{pour} \quad H \end{aligned}$$

Ce système se réduit à $5x + 2z = 4w'$ qui est une équation Diophantienne à trois variables. Par inspection : $x = 2, z = 1, w' = 3$ est une solution correspondant pour laquelle $y' = 2, x' = 1, y = 3, z' = 4$. Cela implique

$$2KMn0_4 + 3H_2SO_4 + H_2O_2 \longrightarrow K_2SO_4 + 2nSO_4 + 4H_2O + 3O_2$$

Dans cet exemple $n' - n = 7 - 5 = 2$. L'équation Diophantienne résultante est de la forme $ax_1 + by_1 = cz_1$ et a $x_1 = cg, \quad y_1 = ck, \quad z_1 = ag + bk, g, k \in \mathbb{N}$ comme solution générale .

3.7.2.2 Formule moléculaire

Supposons qu'une substance de poids moléculaire M contienne deux éléments A et B de poids atomiques a et b. Alors pour une molécule de la substance contenant x atomes de A et y atomes de B,

$$ax + by = M \tag{3.71}$$

où x et y sont des inconnues positives. Pour avoir une équation Diophantienne, a,b et M doivent être entiers. En effet, si I_a et I_b désignent l'entier le plus proche de a et b, et si $a - I_a$ et $b - I_b$ sont si petits pour ces éléments tels que

$$-1/2 < (a - I_a)x + (b - I_b)y < 1/2 \tag{3.72}$$

pour x assez petit pour être trouvé dans la molécule, alors

$$I_a x + I_b y = I_M \tag{3.73}$$

où I_M est l'entier le plus proche de M. L'équation est une équation Diophantienne qui peut

être facilement résolue pour x et y. Si plusieurs ensembles de valeurs positives de x et y satisfont (3.7.2.2), on peut les substituer dans (3.7.2.2) et trouver lequel satisfera (3.7.2.2) au moins avec une erreur minimale (écart par rapport à M). Cet ensemble sera l'ensemble correct de valeurs pour x et y ; c'est-à-dire la solution de l'équation (3.71). De plus, un ensemble de valeurs satisfaisant (3.73) peut contenir un x ou y trop grand pour être raisonnablement attendu pour la taille de la molécule, et peut donc être éliminé pour cette raison. Si plusieurs solutions satisfont l'inégalité (3.7.2.2), alors on procède par élimination. Par exemple, considérons une substance contenant uniquement de l'hydrogène et du soufre avec un poids moléculaire de $66,15$ et nous voulons trouver la formule moléculaire. Si x représente un nombre d'atomes d'hydrogène et y un nombre d'atomes de soufre, alors

$$1.008x + 31,98y = 66.15.$$

Après calcul et vérification, nous avons deux valeurs positives satisfaisant toutes les conditions. Ces solutions sont $(x, y) = \{(34, 1), (2, 2)\}$. On procède maintenant par élimination. Il est très peu probable qu'une molécule de cette taille contienne 34 atomes d'hydrogène (surtout lorsqu'elle contient 1 atome de soufre), cette solution peut être éliminée. Donc $x = 2, y = 2$ et la formule moléculaire est H_2S_2.

Remarque 3.7.1.

Ce raisonnement peut être étendu à une substance contenant plus de deux éléments.

3.7.3 Méthode des équations Diophantiennes et troisième loi de Kepler

En physique par exemple, la méthode d'équation Diophantienne ne traite qu'avec des nombres naturels n. La résolution la plus simple de la troisième loi de Kepler, considérée comme une équation Diophantienne, relative aux trajectoires circulaires de rayons r' et de période t', est

$$\left(\frac{r'}{r}\right)^3 = \left(\frac{t'}{t}\right)^2 = n^6,$$

où r est le rayon et t la période d'une trajectoire singulière. Donc nous avons

$$r' = n^2 r \quad \text{et} \quad t' = n^3 t$$

La relation entre les vitesses est $v' = \dfrac{v}{n}$, de sorte que l'invariant rv^2, qui est dans la gravitation de deux masses m_1 et m_2, égales à $G(m_1 + m_2)$ et en plus :

$$r'v' = nrv$$

qui est la condition quantique qui permet de déterminer les trajectoires privilégiées dans le modèle de Bohr de l'atome d'hydrogène. Et le quantum associé est une nouvelle constante universelle : la constante de Planck. Quelle est donc l'équation Diophantienne qui admet rv comme invariant ? C'est la même équation de Kepler, mais où les exposants principaux sont réduits de un :

$$\left(\frac{r'}{r}\right)^2 = \left(\frac{t'}{t}\right)^1 = n^2.$$

Cette équation est fondamentale, car les exposants s'identifient au nombre de dimensions : 2 pour le plan de la trajectoire, 1 pour le temps. C'est la base du modèle cosmologique à électron unique, basé sur la trajectoire basique et hypothétique de rayon $\lambda_e = \hbar/m_e c$, et de vitesse c :

$$v_n = c/n \quad \text{et} \quad r_n = n\lambda_e$$

Dans cette section, nous avons montré l'application de la méthode mathématique des équations Diophantiennes en Physique et Chimie. Nous pensons que cette méthode peut résoudre de nombreux problèmes non résolus ou partiellement résolus en physique et en chimie. Il serait intéressant de caractériser les différents problèmes non résolus ou partiellement résolus en physique et chimie qui peuvent être abordés par cette méthode. Nous espérons que d'autres chercheurs s'attaquerons à ce problème.

Conclusion

Dans ce travail nous avons considéré le corps des nombres en général, suivi des équations Diophantiennes, où nous avons exploré certaines équations Diophantiennes exponentielles comme les puissances de 2 et 3 qui ont une représentation en somme ou différence des nombres de Fibonacci et Lucas. Toutes ces équations sont des équations Diophantiennes exponentielles. La méthode utilisée pour résoudre ces équations est une double application de la méthode de Baker et de certains calculs avec des fractions continues pour réduire la plage de recherche par force brute pour les variables. Cette méthode combine des arguments élémentaires avec des bornes pour les formes linéaires de logarithmes et des techniques de réduction à partir de l'approximation Diophantienne. Nous avons également montré l'application de la méthode mathématique des équations Diophantiennes en physique et en chimie. Plusieurs articles ont été publiés dans le cadre de cette thèse.

ANNEXE

3.8 Codes Python : New Divisibility Tests

Les codes de cette section viennent d'un article titré **New Divisibility Tests** publié dans Far East Journal of Mathematical Education. Nous avons démontré le nouveau test de divisibilité par 7 découvert par le jeune Nigérian Chika Offili. Nous avons implémenté et comparé dans Python plusieurs test de divisibilité par 7 afin de déterminer le plus effectif. Nous avons également énoncé et démontré un nouveau test de divisibilité par 3. L'idée de rédaction de cet article est née lors d'un échange entre le professeur Ismaïla Diouf et moi pendant ma première visite à l'Université Cheikh Anta Diop de Dakar.

Méthode de Chika pour N1=923456778909811325377849865278365475778276485765351 2536123456789098760774

[52]:
```
from math import floor
def chika(n):
    p=n
    L=len(str(p))
    while L>2:
        p=floor(p//10)-2*(p%10)
        L=len(str(p))
    if p%7==0:
        return True
    else:
        return False
```

```
import timeit
timeTaken=timeit.
 ↪timeit(f'{chika(923456778909811325377849865278365475778276485765
 351253612345678909876077 4)}')
print(timeTaken)
```

```
0.009595800000017013
```

Méthode de Chika pour N2=345267802093647873846901243562721345678902721345637674712 3456789723427234

[53]:
```
from math import floor
def chika(n):
    p=n
    L=len(str(p))
    while L>2:
        p=floor(p//10)-2*(p%10)
        L=len(str(p))
    if p%7==0:
        return True
    else:
        return False

import timeit
timeTaken=timeit.
 ↪timeit(f'{chika(345267802093647873846901243562721345678902721345
 637674712345678972342 7234)}')
print(timeTaken)
```

```
0.009491400000011539
```

Critère pour un grand nombre pour N1=923456778909811325377849865278365475778276485765351253 456789098760774

[54]:
```
def critere_pour_un_grand_nombre(n):
        x=str(n)
        size1=len(x)
```

```
arr=[]
if (size1%3==0):
    for i in range(0,size1,3):
            st=int(x[i:i+3])
            arr.append(st)
elif (size1%3==2):
        arr.append(int(x[0:2]))
        x=x[2:]
        for i in range(0,size1-2,3):
            st=int(x[i:i+3])
            arr.append(st)
else:
        arr.append(int(x[0]))
        x=x[1:]
        for i in range(0,size1-1,3):
                st=int(x[i:i+3])
                arr.append(st)
sum=0
for i in range (len((arr))):
        if i%2==0:
                sum+=arr[i]
        else:
                sum-=arr[i]
r_num=str(abs(sum))
sz=len(r_num)
ans=0
if sz==3:
        s=r_num[0:2]
        ans=int(s)+5*(int(r_num[2]))
else:
        ans=abs(sum)
print(ans)
```

```
import timeit
timeTaken=timeit.
 ↪timeit(f'{critere_pour_un_grand_nombre(923456778909811325377849865278365475778276485765351253612345678909876077 4)}')
print(timeTaken)
```

```
114
0.006870799999887822
```

Critère pour un grand nombre pour N2=345267802093647873846901243562721345678902721345637674712345678972342723 4

[55]:
```
def critere_pour_un_grand_nombre(n):
        x=str(n)
        size1=len(x)
        arr=[]
        if (size1%3==0):
            for i in range(0,size1,3):
                    st=int(x[i:i+3])
                    arr.append(st)
        elif (size1%3==2):
                arr.append(int(x[0:2]))
                x=x[2:]
                for i in range(0,size1-2,3):
                    st=int(x[i:i+3])
                    arr.append(st)
        else:
                arr.append(int(x[0]))
                x=x[1:]
                for i in range(0,size1-1,3):
                        st=int(x[i:i+3])
                        arr.append(st)
        sum=0
        for i in range (len((arr))):
                if i%2==0:
```

```
                        sum+=arr[i]
                else:
                        sum-=arr[i]
        r_num=str(abs(sum))
        sz=len(r_num)
        ans=0
        if sz==3:
                s=r_num[0:2]
                ans=int(s)+5*(int(r_num[2]))
        else:
                ans=abs(sum)
        print(ans)

import timeit
timeTaken=timeit.
 ↪timeit(f'{critere_pour_un_grand_nombre(3452678020936478
738469012435627213456789027213456376747 1 23456789723427234)}')
print(timeTaken)
```

```
1309
0.008285800000521704
```

Méthode du graph pour N1=923456778909811325377849865278365475778276485765351 25361 23456789098760774

[56]:
```
def method_du_graph(n):
    arr=[int(d) for d in str(n)]
    xi=0
    for i in range(len(arr)):
        if arr[i]<7:
            xi+=arr[i]
            xi=xi if xi<7 else xi-7
        else:
            xi+=arr[i]-7
            xi=xi if xi<7 else xi-7
```

```
        if xi==1:
            xi=3
        elif xi==2:
            xi=6
        elif xi==3:
            xi=2
        elif xi==4:
            xi=5
        elif xi==5:
            xi= 1
        elif xi==6:
            xi=4
        else:
            xi=0
    print(xi)



import timeit
timeTaken=timeit.
 ↪timeit(f'{method_du_graph(923456778909811325377849865278365475778276485
 ↪
 653512536123456789098760774)}')
print("Time:", timeTaken)
```

```
3
Time: 0.00700680000045395
```

Méthode du graph pour N2=345267802093647873846901243562721345678902721345637674712345678972342723427234

[57]:
```
def method_du_graph(n):
    arr=[int(d) for d in str(n)]
    xi=0
    for i in range(len(arr)):
        if arr[i]<7:
```

```
            xi+=arr[i]
            xi=xi if xi<7 else xi-7
        else:
            xi+=arr[i]-7
            xi=xi if xi<7 else xi-7
        if xi==1:
            xi=3
        elif xi==2:
            xi=6
        elif xi==3:
            xi=2
        elif xi==4:
            xi=5
        elif xi==5:
            xi= 1
        elif xi==6:
            xi=4
        else:
            xi=0
    print(xi)



import timeit
timeTaken=timeit.
 ↪timeit(f'{method_du_graph(345267802093647873846901243562721345678902721345637674712345678972342723427234)}')
print("Time:", timeTaken)
```

```
0
Time: 0.006731500001478707
```

Méthode de Pascal pour N1=923456778909811325377849865278365475778276485765351253612345678909876077 4

[58]:
```
def Pascal(n):
    st=str(n)
    l=len(st)
    x=[]
    l1=len(x)
    n1=1
    while (l1<l):
        x.append(n1%7)
        n1=10*(n1%7)
        l1=len(x)
    sum=0
    st=st[::-1]
    st=[st[i:i+1] for i in range(0,len(st),1)]
    for i in range (l):
        sum+=int(st[i])*x[i]
    print("Sum: ", sum)
    if(sum%7==0):
        print(n, "is divisible by 7")
    else:
        print(n, "is not divisible by 7")
```

[59]:
```
Pascal(923456778909811325377849865278365475778276485765351253
61234567890987607 74)

import timeit



timeTaken=timeit.
 ↪timeit(f'{Toja(923456778909811325377849865278365475778276485765351253
612345678909876077 4)}')
#output the small multiple of 7 if the number is a multiple of 7
#and the time taken to execute the program
print(timeTaken)
```

```
Sum:  1289
923456778909811325377849865278365475778276485765351253612345678909876077
 ↪is not
divisible by 7
0.019315899999128305
```

Méthode de Pascal pour N2=923456778909811325377849865278365475778276485765351253612345678909876077

[60]:
```
Pascal(345267802093647873846901243562721345678902721345637674712345678972342
7234)

import timeit



timeTaken=timeit.
 ↪timeit(f'{Toja(345267802093647873846901243562721345678902721345637674712345
6789723427234)}')
#output the small multiple of 7 if the number is a multiple of 7
#and the time taken to execute the program
print(timeTaken)
```

```
Sum:  1113
345267802093647873846901243562721345678902721345637674712345678972342723
 ↪is
divisible by 7
0.01432589999967604
```

Méthode de Toja pour N1=923456778909811325377849865278365475778276485765351253612345678909876077

[61]:
```
def Toja(n):
    s=str(n)
    l=len(s)
    x=s
    while l>2:
```

```
        size1=len(x)
        arr=[]
        if (size1%2==0):
            for i in range(0,size1,2):
                st=int(x[i:i+2])
                arr.append(st)
        else:
            arr.append(int(x[0]))
            x=x[1:]
            for i in range (0,size1-1,2):
                st=int(x[i:i+2])
                arr.append(st)
        s=""
        for num in arr:
            x=n//7
            d1=abs(x*7-n)
            d2=abs((x+1)*7-n)
            p=d1 if d1< d2 else d2
            s+=str(p)
        l=len(str(s))
        x=s



import timeit


timeTaken=timeit.
 ↪timeit(f'{Toja(923456778909811325377849865278365475778276485765351253612345678909876074)}')
#output the small multiple of 7 if the number is a multiple of 7
#and the time taken to execute the program
print(timeTaken)
```

```
0.009229600000253413
```

Méthode de Toja pour N2=345267802093647873846901243562721345678902721345637674712345678972342723427234

[62]:
```
def Toja(n):
    s=str(n)
    l=len(s)
    x=s
    while l>2:
        size1=len(x)
        arr=[]
        if (size1%2==0):
            for i in range(0,size1,2):
                st=int(x[i:i+2])
                arr.append(st)
        else:
            arr.append(int(x[0]))
            x=x[1:]
            for i in range (0,size1-1,2):
                st=int(x[i:i+2])
                arr.append(st)
        s=""
        for num in arr:
            x=n//7
            d1=abs(x*7-n)
            d2=abs((x+1)*7-n)
            p=d1 if d1< d2 else d2
            s+=str(p)
        l=len(str(s))
        x=s
    #print(s)


#Toja(5527579818992714771428)
```

```
import timeit


timeTaken=timeit.
 ↪timeit(f'{Toja(345267802093647873846901243562721345678902721345637674712345678972342723
4)}')
#output the small multiple of 7 if the number is a multiple of 7
#and the time taken to execute the program
print(timeTaken)
```

```
0.009436399999685818
```

```
[ ]:
```

```
[ ]:
```

3.9 Codes sources SageMath

Les codes de cette sections viennent de notre article ititulé *On Pillai's problem with Padovan and Pell-Lucas numbers*. Dans cet article, nous avons déterminé les nombres c admettant au moins deux représentations comme différence de nombres de Padovan et Pell-Lucas. En d'autres termes, nous avons résolu l'équation $\mathcal{P}_m - \mathcal{L}_n = c$ où $\mathcal{P}_m$ et $\mathcal{L}_n$ représentent les nombres de Padovan et Pell-Lucas respectivement. Le résultat principal de cet article s'énonce sous forme de théorème comme suit :

Théorème 3.9.1. *The only integers c having at least two representations of the form $\mathcal{P}_m - \mathcal{L}_n$ with $m > 3$ are*

$$c \in \{-2, 1, 2, 3, 7, 10, 14, 15, 31, 35, 80\}.$$

Le tableau suivant donne les couples pour lesquels on obtient les différentes représentations de c sous la forme $\mathcal{P}_m - \mathcal{L}_n = c$.

c	(m,n)
-2	$(6,2),(10,3)$
1	$(5,1),(8,2)$
2	$(6,1),(11,3)$
3	$(7,1),(9,2).(14,4)$
7	$(9,1),(12,3)$
10	$(10,1),(11,2)$
14	$(11,1),(13,3)$
15	$(12,2),(15,4)$
31	$(14,2),(16,4)$
35	$(14,1),(15,3)$
80	$(17,2),(18,4)$

Padovan - PellLucas

Determination of the left and right approximations of the real numbers

[1]:
```
def my_floor(real, n=2):
    f= floor(real*10^n)/10^n
    return f.n(digits=n+1)

def my_ceil(real, n=2):
    c= (floor(real*10^n)+1)/10^n
    return c.n(digits=n+1)
```

Detemination of the polynomial roots

The following cell is the cell of entries

[2]:
```
# Here are the entries you just need to polynomial p1 correspond␣
 ↪the order 2 linear reccurence and p2
# correspond the 3 order linear reccurence and companion mean if␣
 ↪is no if it not the Lucas sequence
p1 = x^2-2*x-1
p2 = x^3-x-1
companion = 'Yes'
```

[3]:
```
if companion == 'No':
    ecart = 4
else:
```

```
    ecart = 3
```

[4]:
```
def myroots(polyx):
    x = var('x')
    if polyx == x^3-x^2-x-1:
        sol1 = solve(x^3-x^2-x-1,x)
        solv1 = [sol_i.rhs() for sol_i in sol1]
        solv1ap = [sol_i for sol_i in solv1]
        return solv1ap
    elif polyx == x^3-x-1:
        sol1 = solve(x^3-x-1,x)
        solv1 = [sol_i.rhs() for sol_i in sol1]
        solv1ap = [sol_i for sol_i in solv1]
        return solv1ap
    else:
        sol1 = solve(polyx,x)
        solv1 = [sol_i.rhs() for sol_i in sol1]
        solv1ap = [sol_i for sol_i in solv1]
        return solv1ap

eta, delta = myroots(p1)
gamma, beta, alp = myroots(p2)

def abc(polyx, companion):
    if polyx == x^3-x-1:
        gamma, beta, alp = myroots(x^3-x-1)
        f(x) = (1+x)/(1+3*x-x^2)
    if polyx == x^3-x^2-x-1:
        gamma, beta, alp = myroots(x^3-x^2-x-1)
        f(x) = 1/(-1+4*x-x^2)
    if polyx != x^3-x-1 and polyx != x^3-x^2-x-1 :
        if companion == 'No':
            eta, delta = myroots(polyx)
```

```
            f(x,y) = 1/(x-y)
            cdelta, ceta = f(delta,eta), f(eta, delta)
            return cdelta, ceta
        else:
            return 1,1
    return f(alp), f(beta),f(gamma)


p, q = abc(p1, companion)
a, b, c = abc(p2, companion)
#somm_coef_ndom_root = 2*((1/(2*sqrt(2)))+nb+nc)
```

[5]:
```
my_floor(abs(alp)), my_ceil(abs(alp))
```

[5]: (1.32, 1.33)

[6]:
```
my_floor(abs(beta)), my_ceil(abs(beta))
```

[6]: (0.860, 0.870)

[7]:
```
my_floor(abs(gamma)), my_ceil(abs(gamma))
```

[7]: (0.860, 0.870)

[8]:
```
my_floor(abs(a)), my_ceil(abs(a))
```

[8]: (0.720, 0.730)

[9]:
```
my_floor(abs(b)), my_ceil(abs(b))
```

[9]: (0.240, 0.250)

[10]:
```
my_floor(abs(c)), my_ceil(abs(c))
```

[10]: (0.240, 0.250)

Relation between n and m

[11]:
```
def cceof(delta, alp):
    nflot = log(delta)/log(alp)
    return ceil(nflot.n())
```

[12]:
```
cf = cceof(delta, alp)
cf
```

[12]: 4

[13]:
```
t = log(alp)/log(delta)
t.n()
```

[13]: 0.319046972208309

Modeling the equation using a dictionary

[14]:
```
coef_dom_root = {
    "delta":p,
    "delta1":-p,
    "eta":q,
    "eta1":-q,
    "alp":-a,
    "alp1":a,
    "beta":-b,
    "beta1":b,
    "gamma":-c,
    "gamma1":c,
}
```

[15]:
```
somm_coef_ndom_root =␣
↪my_ceil(abs(coef_dom_root["eta"]))+my_ceil(abs(coef_dom_root["eta1"]))+my
somm_coef_ndom_root
```

[15]: 3.02

Determination of the constants of the left hand of inequalities

[16]:
```
def intp(a,x):
    return ceil((log(a)/log(x)).n())

def matveev(int_diff, step):
    #first step
```

```
    if step == 'debut':
        coefnm = my_ceil(abs(coef_dom_root["delta1"]))+my_ceil(abs(coef_dom_root["alp1"]))
        coefnmv = [coefnm/(my_floor(abs(a))*my_floor(alp)), coefnm/my_floor(abs(a))]
        exp = [int_diff+my_ceil(log(coefnmv[0])/log(delta),0), my_ceil(log(coefnmv[1])/log(alp),0)]
        return coefnm, coefnmv, exp
    elif step == 'case1':
        coefm = my_ceil(abs(coef_dom_root["alp1"]))+somm_coef_ndom_root
        coefmv = coefm/my_floor(abs(a))
        return coefm, coefmv
    elif step == 'case2':
        coefn = my_ceil(abs(coef_dom_root["delta1"]))+somm_coef_ndom_root
        coefnv = my_ceil(delta)^int_diff*coefn/(my_floor(abs(a))*my_floor(alp))
        return coefn, coefnv
    elif step == 'final':
        coefd = my_ceil(delta)^int_diff*somm_coef_ndom_root/(my_floor(abs(a))*my_floor(alp))
        return coefd
    else:
        return 'stop'
```

[17]:
```
T = ['debut', 'case1', 'case2', 'final']
for i in range(len(T)):
    am = matveev(ecart,T[i])
    print(am)
    if  i == 0:
        deal =  am[2]
    if i == 1:
```

```
        deal1 = am[1]
    if i == 2:
        deal2 = am[1]
    if i == 3:
        deal3 = am
```

```
(4.76, [5.01, 6.61], [5.0, 7.0])
(3.75, 5.21)
(4.03, 60.1)
45.0
```

Determination of the minimal polynomial and of the logarithmic heigh

[18]:
```
def logarithm_heigh(real):
    alg = QQbar(real)
    t = alg.minpoly()
    T=t.coefficients()
    deg = t.degree()
    ce = lcm([t.denominator() for t in T])
    f(x) = ce*t
    Root = f(x).roots(x)
    solv=  [log(max(1,abs(sol_i[0]))) for sol_i in Root]
    R = (1/deg)*(log(ce)+sum(solv))
    return  f, R.n()
```

[19]:
```
if companion == "No":
    real  = (delta-eta)*a
else:
    real = a
out  = logarithm_heigh(real)
out
```

[19]:
```
(x |--> 23*x^3 - 23*x^2 + 6*x - 1, 1.04516473864305)
```

[20]:
```
#matveev lowerbound
import numpy
```

```
def c(s, D):
    return 1.4*30^(s+3)*s^(4.5)*D^2*(1+log(D))

def lower_bound(new, delt, alpha, D,case = 0):
    if case == 3:
        c1 = lower_bound(new, delt, alpha, D,case = 1)[2]
        c2 = lower_bound(new, delt, alpha, D,case = 2)[2]
        Ai = (5/6)*max(c1,c2)
        new = D*max(c1,c2)
        A = [ new , 3*log(delt), 2*log(alpha)]
        s = len(A)
        T = -c(s,D)*numpy.prod(A)
        return my_ceil(Ai), new, my_ceil(-T)
    if case == 1:
        Ai = (1/2)*(lower_bound(new, delt, alpha, D)[2])
        new = D*Ai
        A = [ new , 3*log(delt), 2*log(alpha)]
        s = len(A)
        T = -c(s,D)*numpy.prod(A)
        return my_ceil(Ai), new, my_ceil(-T)
    if case == 2:
        Ai = (1/3)*(lower_bound(new, delt, alpha, D)[2])
        new = D*Ai
        A = [ new , 3*log(delt), 2*log(alpha)]
        s = len(A)
        T = -c(s,D)*numpy.prod(A)
        return my_ceil(Ai), new, my_ceil(-T)
    if case == 0:
        #evl = logarithm_heigh(new)
        r = abs(log(new))
        A1 = max(D*out[1], r.n(), 0.16)
        A = [ A1 , 3*log(delt), 2*log(alpha)]
```

```
        s = len(A)
        T = -c(s,D)*numpy.prod(A)
        return out[1], A1, my_ceil(-T)
```

[21]:
```
D = 6
for i in range(4):
    res = lower_bound(real, delta, alp, D, i)
    print(res)
    if i  == 3:
        Kata = res[2]
```

```
(1.04516473864305, 6.27098843185830, 1.34e14)
(6.71e13, 4.03e14, 8.62e27)
(4.47e13, 2.68e14, 5.74e27)
(7.18e27, 5.17e28, 1.11e42)
```

[ ]:
```
```

Determination of the constants of the right hand of inequalities

[22]:
```
f(x) = x - ecart - Kata*((1+log(1+cf*x))^3)
```

[23]:
```
def resolution(f):
    i = 0
    while  f(10^i) < 0:
        i = i+1
    deb = 10^(i-1)
    fin = 10^i
    t = find_root(f, deb, fin)
    return my_ceil(t)
```

[24]:
```
M = resolution(f)
M
```

[24]:
```
1.61e48
```

Reduction algorithm

[25]:
```
def fct(x,y):
    return int(my_ceil(x,0)+y)
#First = [fct()int(my_ceil(log(2)/
 ↪log(delta),0)+deal[0]),int(my_ceil(log(2)/log(alp),0)+deal[1])]
```

[26]:
```
new_ex = [fct(log(2)/log(delta), deal[0]), fct(log(2)/log(alp),␣
 ↪deal[1])]
Av = [my_ceil(delta^new_ex[0],0),my_ceil(alp^new_ex[1],0)]
```

[27]:
```
first  = continued_fraction(log(delta)/log(alp))
second  = continued_fraction(log(alp)/log(delta))
i=0
while first.denominator(i)< 6*M and second.denominator(i)< 6*M:
    i = i + 1
n_min = i
```

[28]:
```
def dist(real):
    distance = abs(real-round(real))
    return distance.n(prec=1000)
```

[29]:
```
def gd_convergent(mu):
    for i in range(n_min,200):
        de_tau = tau_ex.denominator(i)
        if de_tau > 6*M:
            re = dist(mu * de_tau) - M * dist(tau *  de_tau)
            if re > 0:
                break
    #print('q = q_'+str(i)+' = '+str(de_tau)+' et epsilon =␣
 ↪'+str(re))
    return i, de_tau, re

def borne_superieure_k(A, B, mu):
    i, q, eps = gd_convergent(mu)
    k_sup = ceil(log(A*q/eps)/log(B))
    #print('n < '+str(k_sup))
```

```
    return i, q, eps, k_sup

def printed(input):
    print('q = q_'+str(input[0])+' = '+str(input[1])+' et epsilon␣
 ↪= '+str(input[2])+ ' sup = '+str(input[3]))
```

[30]:
```
tau, mu, A, B = log(delta)/log(alp), -log(real)/log(alp), Av[0],␣
 ↪delta
tau_ex = continued_fraction(tau)
nn11 = borne_superieure_k(A, B, mu)
printed(nn11)
tau, mu, A, B = log(alp)/log(delta), log(real)/log(delta), Av[0],␣
 ↪delta
tau_ex = continued_fraction(tau)
nn12 = borne_superieure_k(A, B, mu)
printed(nn12)
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_87 = 642352593298738180132395389882531829036532711100 24 et␣
 ↪epsilon =
0.0867 sup = 139
```

[31]:
```
tau, mu, A, B = log(delta)/log(alp), -log(real)/log(alp), Av[1],␣
 ↪alp
tau_ex = continued_fraction(tau)
mm11 = borne_superieure_k(A, B, mu)
printed(mm11)
tau, mu, A, B = log(alp)/log(delta), log(real)/log(delta), Av[1],␣
 ↪alp
tau_ex = continued_fraction(tau)
mm12 = borne_superieure_k(A, B, mu)
printed(mm12)
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 424
q = q_87 = 642352593298738180132395389882531829036532711100 24 et␣
 ↪epsilon =
0.0867 sup = 427
```

[32]:
```
nn1 = max(nn11[3], nn12[3])
mm1 = max(mm11[3], mm12[3])
```

[33]:
```
u = var('u')
```

[34]:
```
tau = log(delta)/log(alp)
tau_ex = continued_fraction(tau)
A, B = ceil(2*deal1/log(alp)), alp
mu_alp_m(u) = log((delta^u-1)/real)/log(alp)

outpm11 = borne_superieure_k(A, B, mu_alp_m(1))

for i in range(2,nn1+1):
    out = borne_superieure_k(A, B, mu_alp_m(i))
    if outpm11[3]<out[3]:
        outpm11 = out
    if i%10 == 0:
        printed(out)
printed(outpm11)
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.108
sup = 425
q = q_89 = 104016471548390633532275978348450077320054489242118 et␣
 ↪epsilon =
0.0168 sup = 438
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.418
```

```
sup = 420
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.100
sup = 425
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.135
sup = 424
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.180
sup = 423
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.368
sup = 421
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.126
sup = 425
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0843 sup = 426
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0626 sup = 427
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.00714 sup = 435
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.254
sup = 422
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.320
sup = 421
q = q_89 = 104016471548390633532275978348450077320054489242118 et␣
 ↪epsilon =
```

```
0.0168 sup = 438
```

[35]:
```
tau = log(alp)/log(delta)
tau_ex = continued_fraction(tau)
A, B = my_ceil(2*deal1/log(delta)), alp
mu_del_m(u) = -log((delta^u-1)/real)/log(delta)

outpm12 = borne_superieure_k(A, B, mu_del_m(1))

for i in range(2,nn1+1):
    out = borne_superieure_k(A, B, mu_del_m(i))
    if outpm12[3]<out[3]:
        outpm12 = out
    if i%10 == 0:
        printed(out)
printed(outpm12)
```

```
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.139
sup = 424
q = q_89 = 13008589893497791236506077055105782548576002418529 3 et␣
 ↪epsilon =
0.00806 sup = 437
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.448
sup = 420
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.131
sup = 424
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.166
sup = 424
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.211
```

```
sup = 423
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.398
sup = 420
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.157
sup = 424
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.115
sup = 425
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0932 sup = 426
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0377 sup = 429
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.285
sup = 422
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.351
sup = 421
q = q_89 = 13008589893497791236506077055105782548576002418529 3 et␣
 ↪epsilon =
0.00806 sup = 437
```

[36]:
```
mm = max(outpm11[3], outpm12[3])
```

[37]:
```
tau = log(delta)/log(alp)
tau_ex = continued_fraction(tau)
A, B = ceil(2*deal2/log(alp)), delta
mu_alp_n(u) = log(1/(real*(alp^u-1)))/log(alp)


outpn11 = borne_superieure_k(A, B, mu_alp_m(1))
```

```
for i in range(2,mm1+1):
    out = borne_superieure_k(A, B, mu_alp_m(i))
    if outpn11[3]<out[3]:
        outpn11 = out
    if i%10 == 0:
        printed(out)
printed(outpn11)
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.108
sup = 139
q = q_89 = 104016471548390633532275978348450077320054489242118 et␣
 ↪epsilon =
0.0168 sup = 143
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.418
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.100
sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.135
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.180
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.368
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.126
sup = 139
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0843 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0626 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.00714 sup = 142
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.254
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.320
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0563 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0561 sup = 139
q = q_89 = 104016471548390633532275978348450077320054489242118 et␣
 ↪epsilon =
0.0168 sup = 143
```

[38]:
```
tau = log(alp)/log(delta)
tau_ex = continued_fraction(tau)
A, B = ceil(2*deal2/log(delta)), delta
mu_del_n(u) = -log(1/(real*(alp^u-1)))/log(delta)

outpn12 = borne_superieure_k(A, B, mu_del_m(1))

for i in range(2,mm1+1):
    out = borne_superieure_k(A, B, mu_del_m(i))
    if outpn12[3]<out[3]:
        outpn12 = out
    if i%10 == 0:
        printed(out)
printed(outpn12)
```

```
q = q_87 = 642352593298738180132395389882531829036532711100 24 et␣
 ↪epsilon = 0.139
sup = 138
q = q_89 = 130085898934977912365060770551057825485760024185293 et␣
 ↪epsilon =
0.00806 sup = 142
q = q_87 = 642352593298738180132395389882531829036532711100 24 et␣
 ↪epsilon = 0.448
sup = 137
q = q_87 = 642352593298738180132395389882531829036532711100 24 et␣
 ↪epsilon = 0.131
sup = 139
```

```
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.166
sup = 138
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.211
sup = 138
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.398
sup = 137
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.157
sup = 138
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.115
sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0932 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0377 sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.285
sup = 138
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.351
sup = 137
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0869 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
```

```
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
```

```
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
```

```
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0867 sup = 139
q = q_89 = 13008589893497791236506077055105782548576002418529 3 et␣
 ↪epsilon =
0.00806 sup = 142
```

[39]:
```
nn = max(outpn11[3], outpn12[3])
```

[40]:
```
#var('u,v')
tau = log(alp)/log(delta)
tau_ex = continued_fraction(tau)
A, B = ceil(2*deal3*delta^ecart/log(delta)),delta
mu_del(u,v) =-log((delta^u-1)/(real*(alp^v-1)))/log(delta)

outpnm1 = borne_superieure_k(A, B, mu_del(1,1))

for i in range(1,mm+1):
    for j in range(1,nn+1):
        out = borne_superieure_k(A, B, mu_del(i,j))
        if outpnm1[3]<out[3]:
            outpnm1 = out
```

```
        if i%20 == 0 and j%20 == 0:
            printed(out)
printed(outpnm1)
```

```
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.358
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.364
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.321
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.438
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0715 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0161 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.00116 sup = 147
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.202
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.452
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.378
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0552 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.111
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.126
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.399
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.150
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.106
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.223
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.286
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.231
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.216
```

```
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.176
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.425
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.469
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.352
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0814 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.137
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.152
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.240
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.482
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.439
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.416
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0179 sup = 143
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0732 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0882 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0482 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.298
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.341
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.224
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.209
sup = 141
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.265
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.280
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0116 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0669 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0819 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
```

```
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
```

```
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
```

```
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
```

```
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.246
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.476
```

```
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.432
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon = 0.422
sup = 140
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0114 sup = 144
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0667 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0817 sup = 142
q = q_87 = 64235259329873818013239538988253182903653271110024 et␣
 ↪epsilon =
0.0000143 sup = 152
```

[41]:
```
tau = log(delta)/log(alp)
tau_ex = continued_fraction(tau)
A, B = my_ceil(2*deal3/log(alp),0), delta
mu_alp(u,v) = log((delta^u-1)/(real*(alp^v-1)))/log(alp)

outpnm2 = borne_superieure_k(A, B, mu_alp(1,1))

for i in range(1,mm+1):
    for j in range(1,nn+1):
        out = borne_superieure_k(A, B, mu_alp(i,j))
        if outpnm2[3]<out[3]:
            outpnm2 = out
        if i%20 == 0 and j%20 == 0:
```

```
            printed(out)
printed(outpnm2)
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.327
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.334
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.290
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.407
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0410 sup = 140
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.273
sup = 138
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.458
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.172
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.421
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.446
sup = 137
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.348
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0247 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0800 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0950 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.369
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.119
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0757 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.193
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.256
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.200
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.185
sup = 138
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.146
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.395
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.439
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.322
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0509 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.106
sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.121
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.209
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.452
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.408
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.385
sup = 137
```

```
q = q_87 = 21009447183989024578986011368924076825598287445988 et␣
 ↪epsilon = 0.203
sup = 138
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon =
0.0427 sup = 139
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon =
0.0577 sup = 139
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon =
0.0177 sup = 140
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.267
sup = 138
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.311
sup = 137
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.194
sup = 138
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.179
sup = 138
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.234
sup = 138
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.249
sup = 138
q = q_86 = 20494064998211779897658972120838923421629813452077 et␣
 ↪epsilon = 0.215
sup = 138
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.446
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0364 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0514 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
```

```
q = q_87 = 21009447183989024578986011368924076825598287445988 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 21009447183989024578986011368924076825598287445988 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.216
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.445
sup = 137
```

```
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.402
sup = 137
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon = 0.392
sup = 137
q = q_87 = 210094471839890245789860113689240768255982874459 88 et␣
 ↪epsilon = 0.223
sup = 138
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0362 sup = 140
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0512 sup = 139
q = q_86 = 204940649982117798976589721208389234216298134520 77 et␣
 ↪epsilon =
0.0000610 sup = 148
```

[ ]:

[ ]:

[ ]:

[ ]:

Bibliographie

[1] S. Alaca and K. S.Williams, *Introductory algebraic number theory*, **Cambridge University Press**, 2004.

[2] David Harari, *Algèbre 1-Anneaux et Modules*, notes de cours de Master 1, Université Paris Saclay, 2018.

[3] T. Nagell, *Introduction number theory*, **ALMQVIST & WIKSELL**, 1957.

[4] G. H. Hardy and E. M. Wright. *An introduction to the Theory of Numbers*, **Oxford University Press**, 4th ed., 1960.

[5] I. Niven, H. S. Zuckerman, and H. L.Montgomery, *An introduction to the theory of number*, 5th ed., **JohnWiley and Sons, Inc.**, 1991.

[6] T. Andreescu, D. Andrica, and I. Cucurezeanu, *An introduction to diophantine equations*, **Birkhäusser**, 2010.

[7] E. Zeckendorf, *Représentation des nombres naturels par une somme de nombres ou de nombres de Lucas*, **Bull. Soc. Roy. Sci. Liège** $41(1972), 179 - 182$.

[8] L.J.Mordell,*Diophantine equations*, **Academic Press Inc**, 1969.

[9] H. Cohen, *Number theory*, Vol. II : **Analytic and Modern Tools, Springer,** 2007.

[10] Y. F. Bilu, Y. Bugeaud, and M.Mignotte, *The problem of Catalan*, **Springer International Publishing,** 2014.

[11] C.L. Stewart,*Linear forms in logarithms and diophantine equations*, **Course notes of University of Waterloo taken by D. Wolczuk.**

[12] A. Baker, *Linear forms in the logarithms of algebraic numbers*, iii, **Mathematika** $14(1967)$, pp $220 - 228$.

[13] P. Ribenboim, *My number, my friend*, **popular lecture on number theory, Springer-Verlag**, 2000.

[14] A. Baker and G. Wüstholz, *Logarithm forms and groups varieties*, **J. Reine Angew.Math.** 442(1993), pp. 19 − 62.

[15] A. Baker and G. Wüstholz, *Logarithmic and Diophantine Geometry*, Vol 9 **New Mathematical Monographs (Cambridge University Press)**, 2007.

[16] M. Laurent, M.Mignotte, and Y. Nesterenko, *Formes linéaires de deux logarithmes et déterminant d'interpolation*, **Journal of Number Theory** 55(1995), pp 285 − 321.

[17] F. W. Levi, *On* $a^x + b^y = c$, **J. Indian Math. Soc. (N.S.)** 2(1936), pp. 119 − 122.

[18] F. W. Levi, *A correction to the paper on* $a^x + b^y = c$, **J. Indian Math. Soc.** (N.S.) 2(1937), pp 215.

[19] F. W. Levi, *On the inequality* $0 < a^x - b^y \leq c$, **Journal Indian M. S.** 19(1931), pp. 1 − 11.

[20] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, **Quart. J. Math. Oxford Ser.** 20(1969), 129 − 137.

[21] F. Amoroso et D. Vergnaud, *Minorations de la hauteur d'un nombre algébrique*, **Laboratoire de mathématiques Nicolas Oresme, CNRS UMR 613, Université de Caen** (2002).

[22] A. Baker, *Transcendental Number Theory* **Cambridge University Press**, 1975.

[23] Shorey, T. N. and Tijdeman, R. J. *Exponential Diophantine Equations* **Cambridge University Press**, 1986 ; reprinted 2008).

[24] S. Kebli, O. Kihel, J. Larone, and F. Luca, *On the nonnegative integer solutions to the equation* $F_n \pm F_m = y^a$, **J. Number Theory** 220(2021)107 − 127.

[25] J. J. Bravo and F. Luca, *On the Diophantine equation* $F_n + F_m = 2^a$, **Quaest. Math.** 39(2016), 391 − 400.

[26] E. F. Bravo and J. J. Bravo, *Powers of two as sums of three Fibonacci numbers*, **Lithuanian Mathematical Journal**, (2015).

[27] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations Fibonacci and Lucas perfect powers*, **Ann. of Math.** 163(2006), 969 − 1018.

[28] F. Luca and V. Patel, *On perfect powers that are sums of two Fibonacci numbers*, **J. Number Theory** 189(2018), 90 − 96.

[29] F. Luca, *Repdigits as sums of three Fibonacci numbers*, **Math. Commun.** 17(2012), 1 − 11.

[30] F. Luca and S. Siksek, *Factorials expressible as sums of two and three Fibonacci numbers*, **Proc. Edinb. Math. Soc.** (2)53(2010), 747 − 763.

[31] S. Diaz Alvarado and F. Luca, *Fibonacci numbers which are sums of two repdigits*, **Proceedings of the XIVth International Conference on Fibonacci numbers and their applications (Editors : F. Luca and P. Stanica)**, 2011, 97 − 111.

[32] Milne, James S., *Algebraic number theory* (v3.06), 2014. pages : 164.

[33] Benedict V. N. and Luca F., *Repdigits as Sums of Four Fibonacci or Lucas Numbers*, **Journal of Integer Sequence**, Vol. 21(2018), Article 18.7.7.

[34] L. Debnath, *A short history of the Fibonacci and golden numbers with their applications*, **Int. J. Math. Education Sci. Technology** 42(2011), 337 − 367.

[35] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers*, II, Izv. Ross. Akad. Nauk Ser. Mat. 64(2000), 125 − 180. **Translation in Izv. Math.** 64(2000), 1217 − 1269.

[36] A. Dujella and A. Pethő, *A generalization of a theorem of Baker and Davenport*, **Quart. J. Math. Oxford Ser.** 49(1998), *no*.195, 291 − 306.

[37] Y. Bugeaud, F. Luca, M. Mignotte, and S. Siksek, *Fibonacci numbers at most one away from a perfect power*, Elem. Math. 63(2008), 65 − 75.

[38] J. J. Bravo, F. Luca, and K. Yazán, *On a problem of Pillai with Tribonacci numbers and powers of 2*, **Bull. Korean Math. Soc.** 54.3 (2017), 1069 − 1080.

[39] M. Ddamulira, F. Luca and M. Rakotomalala, *On a problem of Pillai with Fibonacci numbers and powers of 2*, **Proc. Math. Sci.** 127.3 (2017), 411 − 421.

[40] Ddamulira, Mahadi et al. *On a problem of Pillai with k–generalized Fibonacci numbers and powers of 2.* **Monatshefte für Mathematik** 187 (2018) : 635 − 664

[41] J. J. Bravo and F. Lucas, *Powers of Two as Sums of Two Lucas Numbers*, **Journal of Integers sequences**, Vol.17(2014) Article 14.8.3

[42] Boris A. Kordemsky, *The Moscow Puzzles :* 359 *Mathematical Recreations*, **Dover Publications**, p. 140, 2014(1*red*.1971).

[43] Cohen, H. **Number Theory.** Volume I : *Tools and Diophantine Equations* 1st ed. (eds Axler, S. & Ribet, K. A.) (Springer, 2007).

[44] Z. Siar, R. Keskin, *On the Diophantine equation* $F_n - F_n = 2^a$, **Colloq. Math.** 159(2020)119 − 126.

[45] B. Demirtürk Bitim, R. Keskin, *On solutions of the Diophantine equation* $F_n - F_m = 3^a$, **Proc. Indian Acad. Sci. Math. Sci.** 129(2019)81.

[46] Pagdame Tiebekabe and Ismaïla Diouf, *Powers of Three as Difference of Two Fibonacci Numbers*, **JP Journal of Algebra, Number Theory & Applications**, Volume 49, Number 2, (2021), Pages 185 − 196.

[47] F. Erduvan, R. Keskin, *Nonnegative integer solutions of the equation* $F_n - F_m = 5^a$, **Turk. J. Math.** 43(2019)115 − 1123.

[48] I. Pink, V. Ziegler, *Effective resolution of Diophantine equations of the form* $u_n + u_m = wp_1^{z_1} \cdots p_s^{z_s}$, **Monatshefte Math**. 185(2018) 103 − 131.

[49] Edward Brooks, *The Philosophy of Arithmetic*. **Normal Publishing Company**, 1880.

[50] Leonard Eugene Dickson. *History of the Theory of Numbers*. **Chelsea Publishing Company**, (Originally published in 1919 by the Carnegie Institution, Washington, D.C., all three volumes of this text are now available in paperback from Dover Publications, Mineola, NY,2005.), 1952.

[51] Abodah Zarah, *Babylonian Talmud.* **Abod. Zar**. 9b http://come-and-hear.com/zarah/zarah_9.html.

[52] Cherniavsky, Y. and Mouftakhov, A. Zbikowskis *Divisibility Criterion*. **The College Mathematics Journal**, Vol. 45, No. 1 , pp. 17 − 21 ,January (2014).

[53] Dickson, L. E. *History of the theory of numbers.* Vol. I : Divisibility and primality. **Chelsea Publishing Co.**, New York 1966.

[54] Lagrange, J. L. *Leçons élémentaire. sur les math. données à l'école normale* (1795), **Jour. de l'école polytechnique**, vols. 7, 8, 194 − 9 ; Oeuvres, 7, pp. 203 − 8, 1812.

[55] Charles L. Dodgson. *Brief method of dividing a given number by* 9*or*11. **Nature**, 56(1459) : 565 − 566, 1897.

[56] D. H. Lehmer -*Factorization of certain cyclotomic functions*, **Ann. of Math.** 34(1933), *pp*.461 − 479.

[57] A. Zbikowski, *Note sur la divisibilité des nombres*, **Bull. Acad. Imp. Sci. Saint-Pétersbourg** 3151 − 153, 1861.

[58] Marc Renault. *Stupid divisibility tricks : 101 ways to stupefy your friends*. **Math Horizons**, 14(2) : 18 − 21, 42, November 2006.

[59] Pagdame Tiebekabe and Ismaïla Diouf, *Powers of Three as Difference of Two Fibonacci Numbers*, **JP Journal of Algebra, Number Theory & Applications**, Volume 49, Number 2, (2021), Pages 185 − 196. http ://dx.org/10.17654/NT049020185.

[60] Pagdame Tiebekabe and Ismaïla Diouf, *New Divisibility Tests*, **Far East Journal of Mathematical Education**, Volume 21, Number 1, (2021), Pages 31 − 41. http ://dx.doi.org/10.17654/ME021010031.

[61] P. Tiebekabe and I. Diouf, *On solutions of the Diophantine equation* $L_n + L_m = 3^a$, **Malaya J. Mat.** 9(04)(2021), 228 − 238. http ://doi.org/10.26637/mjm904/007.

[62] Pagdame Tiebekabe and Ismaïla Diouf, *Linear forms in Logarithms and the mathematical method of Diophantine equations : Applications in Chemistry and Physics*, **Journal of Mathematical Chemistry**, https ://doi.org/10.1007/s10910-021-01274-y, Volume 59, (2021), Pages 2009 − 2020.

[63] P. Tiebekabe and I. Diouf, *On solutions of Diophantine equation* $F_{n_1} + F_{n_2} + F_{n_3} + F_{n_4} = 2^a$, **Journal of Algebra and Related Topics**, Volume 9, Issue 2, 131 − 148(2021) https ://doi.org/10.22124/JART.2021.19294.1266.

RÉSUMÉ

Nom et prénom du candidat : **Pagdame TIEBEKABE**

Formes linéaires de logarithmes et équations Diophantienne

Le domaine de la transcendance a une variété de sous-domaines comprenant : la transcendance des nombres individuels, l'indépendance algébrique, la transcendance des fonctions (par exemple, les formes modulaires, les fonctions zêta et j, etc.) à des valeurs particulières, et les applications aux équations Diophantiennes qui impliquent les suites récurrentes linéaires (par exemple, les nombres de Fibonacci, les nombres de Lucas, les nombres de Tribonacci, les nombres de Padovan et les nombres de Pell-Lucas). Dans ce travail, nous avons considéré le corps des nombres en général, suivi des équations Diophantiennes, où nous avons exploré quelques équations Diophantiennes exponentielles en suites récurrentes linéaires. La méthode utilisée pour résoudre ces équations est une double application de la méthode de Baker et de quelques calculs avec des fractions continues. Elles combinent des arguments élémentaires avec des bornes pour les formes linéaires de logarithmes et techniques de réduction à partir de l'approximation Diophantienne. Nous avons également montré l'application de la méthode mathématique des équations Diophantiennes en physique et chimie.

ABSTRACT

Full Name of the candidate : **Pagdame TIEBEKABE**

Linear forms in Logarithms and Diophantine equation

The field of transcendance has a variety of subfields including : the transcendence of individual numbers, algebraic independence, transcendence of functions (for example, modular forms, the zeta and j functions, etc.) at particular values, and applications to Diophantine equations which involve the linearly recurrent sequences (for example, Fibonacci numbers, Lucas numbers, Tribonacci numbers, Padovan numbers, and the Pell-Lucas numbers). In this work we have considered the number field in general, followed by the Diophantine equations, where we have explored some exponential Diophantine equations in linearly recurrent sequences. The method used to solve these equations is a double application of Baker's method and some computations with continued fractions to reduce the brute force search range for the variables. They combine elementary arguments with bounds for linear forms in logarithms and reduction techniques from the Diophantine approximation. We have also shown the application of the mathematical method of Diophantine equations in physics and chemistry.