N d'ordre :**196/2024-C/MT**

République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

FACULTÉ DE MATHÉMATIQUES

THÈSE DE DOCTORAT

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

En : MATHÉMATIQUES

Spécialité : Arithmétique Codage et Combinatoire

Par : Zahra AMEUR

Sujet :

Etude de certaines Equations Diophantiennes Exponentielles

Soutenue publiquement le mercredi 26 juin 2024, devant le jury composé de :

M. B.BENSEBA	**Professeur à l'USTHB**	**Président**
M. T.GARICI	**Maître de conférences/A à l'USTHB**	**Directeur de thèse**
M. B.FARHI	**Professeur à l'ENSM, Sidi-Abdellah**	**Examinateur**
M. M.HERNANE	**Professeur à l'USTHB**	**Examinateur**
M. S.RIHANE	**Maître de conférences/A à l'ENSM, Sidi-Abdellah**	**Examinateur**
M. R.BOUMAHDI	**Maître de conférences/A à l'ENSM, Sidi-Abdellah**	**Invité**

12 juillet 2024

Dédicaces

Je dédie ce travail aux membres de ma famille et à mes amies, dont le soutien indéfectible a été une source de force et d'inspiration.

Je voudrais commencer par exprimer ma profonde gratitude envers mes très chers parents pour leur amour inconditionnel, leur soutien constant et leurs sacrifices sans fin. Leur encouragement et leur confiance en moi ont été les fondements sur lesquels j'ai construit mon parcours académique. Sans eux je ne serai jamais arrivée là où je suis aujourd'hui. Je tiens particulièrement à remercier ma sœur Louiza, qui malgré son jeune âge, m'a toujours soutenu et encouragée. Son soutien indéfectible et sa foi en moi ont été des sources d'inspiration inestimables. Je lui serai éternellement infiniment reconnaissante. Je souhaite également exprimer ma gratitude envers mes deux frères, Mokrane et Abderrahim Saleh. Leur présence et leur soutien ont été d'une valeur inestimable tout au long de ce parcours, et je leur suis reconnaissante pour leur amour et leur encouragement constants. De plus, je tiens à souligner que c'est mon grand frère Mokrane qui m'a conseillé de choisir la spécialité mathématiques au lycée. Je le remercie pour ce précieux conseil, car c'est finalement dans cette spécialité que je me suis épanouie le plus.

Je tiens également à exprimer ma profonde gratitude envers mes cousines et cousins, Fatma, Nora, Fatiha, Samira, Smail, Abdallah et Samir, ainsi que mes tantes Aicha et Nassima, pour leur présence et leurs encouragements constants. Leur soutien indéfectible a été une source d'inspiration inestimable, et je leur suis infiniment reconnaissante pour leur soutien sans faille. Je souhaite également remercier tonton Mustapha, nena Fouzia, Ratiba et Fatma Zohra pour leur amour et encouragements. Je souhaite exprimer mes vœux les plus sincères de bonheur et de réussite à leurs enfants, Meriem, Lyna, Mohamed, Tarek, Tahar, Amira, Rima, Adem, Sofia, Nessrine et Wassim.

À mon amie d'enfance Zineb Bouallaga, et à mon amie depuis le lycée, ma sœur Sabrina Nechab, je vous dédie ce travail avec une profonde gratitude pour tout ce que vous avez fait pour moi. Que Dieu vous garde à mes côtés. Merci d'être toujours présentes. À mon amie de l'ESI, Imene Allalou. À mes amies depuis licence mathématiques, Assia Krimat, Hadjer Beldjoudi, Yasmina Hamma, Katia Benseba, Kenza Abdelguerfi, Rym Smai et Fatiha Sadouki.

Chacune d'entre vous a joué un rôle essentiel dans ma vie, que ce soit sur le plan personnel ou académique. Votre soutien inconditionnel et vos conseils précieux ont été d'une aide précieuse tout au long de notre parcours commun. Je me considère extrêmement chanceuse de vous avoir comme amies. Pour tout ce que vous avez fait pour moi, je vous serai reconnaissante pour toujours. En particulier, à Hadjer Beldjoudi et Katia Benseba, je n'oublierai jamais les deux années de master que nous avons passées ensemble. Toutes les discussions de mathématiques que nous avons eues étaient enrichissantes. Sans votre compagnie, le master ACC n'aurait pas été l'une des meilleures expériences de ma vie.

À Sarra Kentache, Imen Khettabi, Amina Boutelba, Kechiche Dounya, Chahinez Imine, Chahinez Djadi, Hayet Bensella, Meriem Tiachachat, Lachemi Nadia, Safia Seffah, Khadidja Moussaoui, Fatima Zohra Bensaci et Boucherikha Ahlem. Ma formation doctorale n'aurait pas été aussi enrichissante sans votre présence. Les moments que nous avons partagés ensemble, que ce soit au CAM ou à la Bibliothèque, resteront gravés dans ma mémoire. Je vous remercie du fond du cœur pour votre soutien et votre amitié tout au long de cette période. Sarra, je n'oublierai jamais notre première rencontre à la bibliothèque centrale en 2017 et tes conseils qui m'ont beaucoup aidé. Imen je te serai toute ma vie reconnaissante pour tout ce que tu as fait pour moi depuis que nous nous sommes rencontrés en master. Amina et Chahinez Imine, je n'oublierai jamais les moments que nous avons passés à la BN cet été. Vos encouragements pendant cette période décisive dans la rédaction de ma thèse ont été d'une importance capitale. Je vous serai éternellement reconnaissante. Dounya et Amina, je vous remercie pour tout ce que vous avez pu faire pour moi, votre présence a été très importante dans certains moments très difficiles. Je vous remercie aussi pour toutes les discussions de maths que nous avons eues et qui ont été enrichissantes. Je tiens également à exprimer ma gratitude envers Chahinez Djadi pour avoir pris le temps de lire ma thèse et pour les remarques précieuses qui ont contribué à améliorer sa version finale. Je voudrais remercier Meriem Tiachachat, Meriem Moulay et Lamia Zerfa pour leurs conseils précieux concernant l'enseignement et pour avoir partagé leur expérience en tant qu'enseignantes avec moi. Enfin, je ne saurais oublier mes amies Besma Yettou, Fatma Bouzidi, Chahinez Mensouri et ma voisine Lamia Dechouk, pour leur encouragements et tout ce qu'elles ont pu faire pour moi.

Remerciements

Je tiens à exprimer ma profonde gratitude envers mon directeur de thèse, le Professeur Tarek GARICI, pour son encouragement et son soutien exceptionnel tout au long de mon parcours doctoral. Sa disponibilité sans faille et sa générosité intellectuelle ont été remarquables. Toujours présent pour répondre à mes questions et surmonter les obstacles, il n'a pas hésité à travailler avec moi, même pendant les périodes de vacances, pour perfectionner notre article et faire avancer ma thèse. Je lui suis infiniment reconnaissante pour le temps précieux qu'il m'a consacré avec patience et dévouement. Ses conseils éclairés sur la rédaction d'articles scientifiques, de thèses et même de cours ont été d'une valeur inestimable pour moi. De plus, son expertise en LaTeX m'a été d'une grande utilité. Le Professeur GARICI m'a initiée au monde fascinant des fractions continues, des équations diophantiennes et des formes linéaires en logarithmes, enrichissant ainsi mes connaissances mathématiques. Avant même d'être mon directeur de thèse, j'ai eu la chance de bénéficier de ses enseignements lors de cours sur les corps finis et le codage en Master 1 et 2. Son approche rigoureuse et sa façon d'aborder les problèmes mathématiques ont profondément influencé ma manière de penser et de travailler. Je le remercie également de m'avoir donné l'opportunité de prendre les travaux dirigés de plusieurs cours qu'il enseignait, enrichissant ainsi mes connaissances mathématiques et développant ma capacité à enseigner. Je suis profondément influencée par sa méthode d'enseignement, sa clarté dans les explications et sa passion pour les mathématiques. Tout cela constitue une base solide pour mes futures recherches et mon engagement en tant que chercheuse et enseignante. Pour tout cela, je lui exprime ma sincère reconnaissance et mon profond respect. Cette expérience a été inestimable pour mon développement académique et personnel.

Je souhaite exprimer ma profonde gratitude envers le Professeur Rachid BOUMAHDI, qui a collaboré avec nous sur notre article. Monsieur BOUMAHDI, a été mon professeur du module algèbre à l'ESI, puis à nouveau mon enseignant du module extensions de corps en Master 1, un module que j'ai particulièrement apprécié et que j'utilise régulièrement. Professeur BOUMAHDI a toujours été une source d'encouragement pour moi. C'est grâce à lui que j'ai développé le désir de poursuivre mes études et de faire un doctorat. Il a profondément modifié ma perspective et a orienté positivement tout mon parcours académique.

Monsieur BOUMAHDI m'a non seulement encouragée à atteindre mes objectifs, mais il m'a également redonné confiance en moi. Ses conseils éclairés et ses encouragements constants ont été des piliers essentiels tout au long de mon parcours. De plus, je tiens à souligner la générosité du Professeur BOUMAHDI. En prenant le temps de lire ma thèse et de me fournir des commentaires précieux, il a grandement contribué à l'amélioration de sa version finale. Son expertise et son attention aux détails ont été d'une valeur inestimable pour moi. Tout ce que je pourrais faire pour exprimer ma reconnaissance envers le Professeur BOUMAHDI ne saurait égaler l'impact profond qu'il a eu sur ma vie académique. Pour toutes ces raisons, je lui serai éternellement reconnaissante.

Travailler avec les Professeurs BOUMAHDI et GARICI a été une expérience enrichissante, et je serai ravie de travailler avec eux à l'avenir. Je les remercie pour tout ce qu'ils ont pu m'apprendre. J'ai été honorée de travailler à leurs côtés.

Je tiens également à remercier respectueusement le Professeur Boualem BENSEBA pour m'avoir fait l'honneur de présider le jury de cette thèse. Monsieur BENSEBA a joué un rôle essentiel dans mon parcours académique en m'enseignant deux modules très importants en Master 1 et 2. Grâce à lui, j'ai découvert la théorie de Galois ainsi que l'arithmétique dans les corps des nombres. La théorie de Galois m'a particulièrement captivée, et elle reste mon module préféré jusqu'à présent. Je me souviens d'un cours particulièrement détaillé et bien expliqué. Je voudrais également le remercier pour ses encouragements et lui exprimer ma reconnaissance pour tout ce qu'il a fait pour moi.

Je souhaiterais témoigner mon plus profond respect et mon infinie gratitude aux Professeurs *Bakir FARHI*, *Mohand Ouamer HERNANE* et *Salah Eddine RIHANE*, pour avoir eu la gentillesse et d'avoir bien voulu accepter d'examiner ce travail

Je tiens à exprimer ma profonde gratitude envers les enseignants qui ont joué un rôle déterminant dans mon parcours académique, en particulier ceux de licence mathématiques et master ACC. Leurs enseignements et leur soutien ont grandement contribué à forger ma passion pour les mathématiques.

Tout d'abord, je souhaiterais adresser mes plus sincères remerciements à Monsieur Mourad ABCHICHE, qui a été mon professeur d'algèbre pendant les deux années de licence en mathématiques. C'est grâce à son cours remarquablement structuré et à son talent pour expliquer les concepts complexes que j'ai développé un véritable amour pour l'algèbre. Son engagement envers ses étudiants et ses encouragements tout au long de ma formation doctorale ont été d'une valeur inestimable pour moi. Je lui serai toujours reconnaissante pour son influence positive sur mon parcours académique et pour le soutien qu'il m'a apporté.

Je voudrais également exprimer ma reconnaissance envers Madame Djamila OUDRAR, qui a été ma professeure d'algèbre pendant une petite période lors de ma troisième année licence en mathématiques. Son enseignement et ses encouragements ont été d'une grande aide pour moi.

Je souhaite également adresser mes remerciements à Monsieur Khaled M'HAMED MESSAOUD, mon professeur des modules Analyse 3 et Analyse 4. Sa passion pour les mathématiques et son soutien constant, notamment en me fournissant des livres pertinents, ont joué un rôle crucial dans mon développement académique, en particulier lors de la réalisation de mon mémoire de licence. Sa générosité et son dévouement envers ses étudiants ont été une source d'inspiration pour moi, et je lui suis profondément reconnaissante pour tout ce qu'il a fait pour moi.

Je souhaite remercier Monsieur Redha CHELLAL, mon professeur d'analyse complexe en Master 1, pour son enseignement inspirant et ses encouragements tout au long de ma formation doctorale. Sa manière de nous pousser vers l'avant a été très appréciée. Je lui suis profondément reconnaissante pour son soutien continu.

Je tiens à remercier chaleureusement Madame Nawel KAHOUL, ma professeure du module complexité algorithmique. Grâce à ses explications claires, j'ai beaucoup appris. Elle a toujours été gentille avec moi et m'a donné de précieux conseils. Sa bienveillance et son soutien m'ont beaucoup aidé. Pour tout cela je lui serai toujours reconnaissante.

Enfin, un immense merci à Monsieur Rachid BOUCHENNA, qui a été mon professeur en master 1 des modules Anneaux et modules 1 et 2. Ses cours approfondis sur les anneaux et les modules m'ont non seulement permis d'acquérir une compréhension approfondie de ces sujets, mais aussi de développer ma capacité à raisonner de manière rigoureuse et à rédiger de façon claire et précise. Son encadrement lors de mon mémoire de master, où nous avons travaillé sur la théorie de Galois dans le cas fini et le cas infini, a été une expérience enrichissante qui a façonné ma compréhension des liens entre l'algèbre et la topologie. Je suis également profondément reconnaissante pour le soutien et les encouragements constants que Monsieur BOUCHENNA m'a prodigué tout au long de mes études.

Table des matières

Notations

1. $\mathbb{N} = \{0, 1, 2, \ldots\}$: l'ensemble des entiers naturels.
2. $\mathbb{N}^* = \{1, 2, \ldots\}$: l'ensemble des entiers naturels non nuls.
3. $\mathbb{Z}$: l'ensemble des entiers rationnels.
4. $\mathbb{Q}$: l'ensemble des nombres rationnels.
5. $\mathbb{F}_p$: le corps fini à p élément.
6. $\mathbb{F}_{p^n}$: le corps fini à p^n éléments.
7. $\overline{\mathbb{F}_p}$: la clôture algébrique de $\mathbb{F}_p$.
8. $\mathbb{F}_{p^n}^*$: le groupe multiplicatif de $\mathbb{F}_{p^n}$.
9. $\nu_p(n)$: la valuation p-adique de l'entier n. C'est la plus grande puissance de p qui divise n.
10. $\lfloor x \rfloor$: la partie entière d'un nombre réel x, i.e. l'unique entier rationnel k vérifiant : $x - 1 < k \leqslant x$.
11. Si $a, b \in \mathbb{Z}$, $[\![a, b]\!] = \{k \in \mathbb{N} \mid a \leqslant k \leqslant b\}$.
12. $\{x\}$: la partie fractionnaire d'un nombre réel x.
13. $\left(\frac{n}{p}\right)$: le symbole de Legendre.
14. $T_k(X)$: Le k-ième polynôme de Tchebychev de première espèce.
15. $U_k(X)$: Le k-ième polynôme de Tchebychev de seconde espèce.
16. $\mathbb{M}_2(\mathbb{Z})$: l'ensemble des matrices carrées d'ordre deux à coefficients entiers.

Introduction

Les équations diophantiennes représentent l'un des domaines les plus intéressants de la théorie des nombres. Ce sont des équations dont les solutions sont cherchées parmi les nombres entiers ou rationnels. C'est souvent des équations polynomiales à coefficients entiers, dont la résolution peut parfois être simple, mais d'autres fois, peut être extrêmement complexe. Parmi les outils utilisés pour étudier ces équations, on trouve les congruences, les résidus quadratiques et les fractions continues.

Il existe un autre type d'équations diophantiennes, appelées équations diophantiennes exponentielles. Ce sont des équations dont au moins l'une des inconnues se trouve en exposant. Par exemple, l'équation $2^n - 3^m = 5$ qui admet uniquement deux solutions $(m, n) = (3, 1)$ et $(m, n) = (5, 3)$ dans $\mathbb{N}^2$. Cette dernière semble élémentaire, mais sa résolution nécessite l'utilisation de la méthode de Baker basée sur les formes linéaires en logarithmes.

Dans cette thèse, nous nous sommes intéressés à l'étude des équations diophantiennes exponentielles

$$(a^n - 1)(b^n - 1) = x^2 \tag{1}$$

et

$$(a^n - 1)(b^m - 1) = x^2, \tag{2}$$

où $(n, m, x) \in \mathbb{N}^* \times \mathbb{N}^* \times \mathbb{N}^*$ sont des inconnues, et a et b sont deux entiers distincts et strictement supérieurs à 1. Depuis l'an 2000, de nombreuses études ont porté sur l'équation (1). Le premier à s'y intéressé est Szalay [18], il a prouvé en 2000 que cette équation n'a pas de solutions en entiers strictement positifs n et x pour $(a, b) = (2, 3)$. Il a également prouvé que le couple $(n, x) = (1, 2)$ représente l'unique solution de l'équation $(2^n - 1)(5^n - 1) = x^2$. Dans la même année Hajdu et Szalay [7] ont prouvé que l'équation $(2^n - 1)(6^n - 1) = x^2$ n'a pas de solutions en entiers strictement positifs n et x. Ils ont aussi étudié l'équation $(a^n - 1)(b^n - 1) = x^2$ pour $b = a^k$ avec $k > 1$ et $kn > 2$. Ils ont montré que dans ce cas les solutions sont les suivantes : $(a, n, k, x) = (2, 3, 2, 21)$, $(3, 1, 5, 22)$, $(7, 1, 4, 120)$. En 2002, Cohn [5] a prouvé que si n est un multiple de 4, alors l'équation (1) n'a de solutions que lorsque $n = 4$ avec $\{a, b\} = \{13, 239\}$. Il a conjecturé aussi que l'équation diophantienne $(a^n - 1)(b^n - 1) = x^2$ n'a pas de solutions en entiers strictement positifs n et x pour $n > 4$. De plus, il a montré que $n = 2$ si et seulement si il existe des entiers positifs r, s et c tels que $a = T_r(c)$, $b = T_s(c)$ et $x = (c^2 - 1)U_{r-1}(c)U_{s-1}(c)$, où T_k et U_k sont les k-ème polynômes de Tchebychev de première et seconde espèce respectivement. Ces derniers peuvent être définis par $T_0 = U_0 = 1$, $T_1 = \frac{1}{2}U_1 = X$, et pour tout entier $k \geqslant 0$,

$T_{k+2} = 2XT_{k+1} - T_k$ et $U_{k+2} = 2XU_{k+1} - U_k$.

Depuis, plusieurs auteurs se sont intéressés à l'étude de l'équation (1) sous différentes hypothèses sur a et b. Nous pouvons citer Le [12], Lan et Szalay [11], Tang [19], Noubissie et al [16] et Noubissie et Togbé [15]. En résumé, ils ont respectivement démontré que l'équation (1) n'a pas de solution en entiers strictement positifs n et x si l'une des conditions suivantes est vérifiée.

— $a = 2$ et $b \equiv 0 \pmod 3$,
— $a \equiv 2 \pmod 6$ et $b \equiv 0 \pmod 3$,
— $a \equiv 0 \pmod 2$ et $b \equiv 15 \pmod{20}$,
— $a \equiv 0 \pmod 2$, b est premier et $b \equiv 3 \pmod 8$,
— $a \equiv 0 \pmod 2$ et $b \equiv 3 \pmod{12}$.

En 2016, en utilisant les solutions de l'équation diophantienne $u^2 - dv^2 = 1$, où d est un entier strictement positif et non carré (connue sous le nom d'équation de Pell-Fermat), Ishii [8] a donné une condition nécessaire et suffisante pour l'existence de solutions pour l'équation (1) dans le cas où $a \equiv 5 \pmod 6$ et $b \equiv 0 \pmod 3$. Inspirés par ce résultat, Noubissie et Togbé ont donné une condition nécessaire et suffisante pour l'existence de solutions pour l'équation (1) dans le cas où $a \equiv 4 \pmod 5$ et $b \equiv 0 \pmod 5$.

Revenons à l'an 2000, en cette année, Walsh [22] a traité l'équation diophantienne exponentielle (2). Il a prouvé que cette dernière n'a pas de solutions en entiers strictement positifs n, m et x pour $(a, b) = (2, 3)$. En 2011, Tang [19] a amélioré ce résultat en prouvant que l'équation (2) n'a pas de solutions lorsque $a \equiv 2 \pmod 6$ et $b \equiv 3 \pmod{12}$.

Récemment, conjointemant avec Boumahdi et Garici [1], avons amélioré les résultats sus-cités concernant les équations diophantiennes (1) et (2). Pour cela, nous avons utilisé quelques propriétés concernant les solutions de l'équation de Pell-Fermat, leur lien avec les polynômes de Tchybychev de première et seconde espèce, ainsi que d'autres résultats provenant des travaux de Cohn [5], Van Der Waal [21] et Bennet [3]. Nous avons par exemple montré que si a est pair, $b \equiv 3 \pmod 4$ et b possède un facteur premier $p \equiv \pm 3 \pmod 8$, alors l'équation (1) n'a pas de solutions en entiers strictement positifs n et x. Nous avons également examiné le cas où $a^2 \equiv -1 \pmod p$ et $p \equiv 1 \pmod 8$ est un facteur premier de b. Nous avons prouvé que si l'équation (1) admet une solution alors n est pair.

Cette thèse est organisée en trois chapitres. Le premier chapitre est consacré à l'étude du développement en fraction continue d'un nombre réel. En particulier, le développement en fraction continue d'un irrationnel quadratique $\sqrt{d}$, où d est un entier strictement positif et non carré, un outil très utile à la résolution de l'équation de Pell-Fermat $u^2 - dv^2 = 1$. Dans le second chapitre, nous nous concentrons sur l'étude de certaines propriétés des solutions de l'équation de Pell-Fermat $u^2 - dv^2 = 1$. Nous montrons que cette dernière admet une infinité de solutions en entiers positifs (x_k, y_k) et nous donnons un lien entre (x_k, y_k) et les polynômes de Tchebychev de première et seconde espèce. Nous clôturons ce chapitre par présenter quelques nouveaux résultats indispensables aux preuves des résultats du dernier chapitre, concernant l'indice de divisibilité $h(p)$ dans la suite $(x_k)_{k\in\mathbb{N}}$, où p est un nombre premier. Ce dernier correspond au plus petit h vérifiant $x_h \equiv 0 \pmod p$. Dans le troisième

et dernier chapitre, nous présentons nos nouveaux résultats [1] concernant les équations diophantiennes (1) et (2). Nous donnons par exemple une condition nécessaire et suffisante pour l'existence de solutions pour l'équation (1) lorsque $p \equiv \pm 3 \pmod 8$, $a \equiv -1 \pmod p$ et $b \equiv 0 \pmod p$.

Chapitre 1

Fractions continues

Les fractions continues sont un concept fascinant qui trouve son utilisation dans divers domaines, tel que la théorie des nombres. Cette notion est définie comme étant une expression de la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

notée $[a_0, a_1, \ldots, a_n]$, ou de la forme

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}},$$

notée $[a_0, a_1, a_2, \ldots]$, où $a_0 \in \mathbb{Z}$ et les a_n sont des entiers strictement positifs. Les fractions continues ont des propriétés intéressantes qui les rendent particulièrement utiles dans la résolution d'équations diophantiennes telles que les équations de Pell-Fermat.

Dans ce chapitre, nous nous intéressons à l'étude du développement en fraction continue d'un nombre réel. En particulier, à celui des nombres irrationnels. On dit qu'un irrationnel x admet un développement en fraction continue s'il existe un entier a_0 et une suite d'entiers strictement positifs $(a_n)_{n\geqslant 1}$ tels que

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

L'un des principaux résultats de ce chapitre est que tout nombre irrationnel admet un développement en fraction continue, et ce dernier est unique. Noter que pour tout entier $n \geqslant 0$, le rationnel $[a_0, \ldots, a_n]$ est appelé réduite d'ordre n de x. Une question naturelle consiste à savoir sous quelle condition suffisante un nombre rationnel $\frac{p}{q}$ figure parmi les réduites de x. La réponse à cette question a été donnée par Andrien-Marie Legendre en 1798 en prouvant

que si $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, alors $\frac{p}{q}$ est une réduite de x. Grâce à ce résultat nous démontrons dans le prochain chapitre que si d est un entier strictement positif et non carré et si u, v vérifient $u^2 - dv^2 = 1$ alors $\frac{u}{v}$ est une réduite de $\sqrt{d}$. Nous clôturons ce chapitre par donner des résultats concernant la périodicité du développement en fraction continue des nombres irrationnels quadratiques, dûs à Leonhard Euler, Joseph-Louis Lagrange et Evariste Galois.

Pour ce chapitre, nous nous sommes inspirés des livres suivants : [2], [9], [17] et [20].

1.1 Fractions continues : Définitions et généralités

Nous débutons notre étude par définir la suite de fractions rationnelles $(F_n)_{n\geqslant 0}$ par récurrence de la manière suivante :

$$F_0(X_0) = X_0, \tag{1.1}$$

et pour tout $n \geqslant 0$,

$$F_{n+1}(X_0, \ldots, X_{n+1}) = F_n\left(X_0, \ldots, X_{n-1}, X_n + \frac{1}{X_{n+1}}\right). \tag{1.2}$$

Calculons les termes F_1 et F_2 :

— Pour $n = 1$, nous avons

$$\begin{aligned} F_1(X_0, X_1) &= F_0\left(X_0 + \frac{1}{X_1}\right) \\ &= X_0 + \frac{1}{X_1} \qquad (1.3) \\ &= \frac{X_0X_1 + 1}{X_1}. \qquad (1.4) \end{aligned}$$

— Pour $n = 2$, nous avons

$$\begin{aligned} F_2(X_0, X_1, X_2) &= F_1\left(X_0, X_1 + \frac{1}{X_2}\right) \\ &= \frac{X_0\left(X_1 + \frac{1}{X_2}\right) + 1}{X_1 + \frac{1}{X_2}} \\ &= \frac{X_2(X_0X_1 + 1) + X_0}{X_2X_1 + 1}. \qquad (1.5) \end{aligned}$$

Nous remarquons que

$$F_1(X_0, X_1) = X_0 + \frac{1}{X_1}.$$

Nous pouvons facilement vérifier que :

$$F_2(X_0, X_1, X_2) = X_0 + \cfrac{1}{1 + \cfrac{1}{X_2}}.$$

D'une manière générale, nous avons

$$F_n\left(X_0, \ldots, X_n\right) = X_0 + \cfrac{1}{X_1 + \cfrac{1}{\ddots X_{n-1} + \cfrac{1}{X_n}}}.$$

Proposition 1.1. *Pour tout entier $n \geqslant 0$,*

$$F_{n+1}(X_0, \ldots, X_{n+1}) = X_0 + \frac{1}{F_n(X_1, \ldots, X_{n+1})}.$$

Démonstration.

— En utilisant (1.3) suivie de (1.1) nous obtenons : $F_1(X_0, X_1) = X_0 + \frac{1}{F_0(X_1)}$. Ainsi, la relation est vérifiée pour $n = 0$.

— Fixons $n \geqslant 0$. Supposons que

$$F_{n+1}(X_0, \ldots, X_{n+1}) = X_0 + \frac{1}{F_n(X_1, \ldots, X_{n+1})}.$$

et montrons que

$$F_{n+2}(X_0, \ldots, X_{n+2}) = X_0 + \frac{1}{F_{n+1}(X_1, \ldots, X_{n+2})}.$$

En utilisant la relation (1.2), nous obtenons

$$F_{n+2}(X_0, \ldots, X_{n+2}) = F_{n+1}\left(X_0, \ldots, X_n, X_{n+1} + \frac{1}{X_{n+2}}\right).$$

En utilisant maintenant l'hypothèse de récurrence, nous obtenons

$$F_{n+2}(X_0, \ldots, X_{n+2}) = X_0 + \frac{1}{F_n\left(X_1, \ldots, X_{n+1} + \frac{1}{X_{n+2}}\right)}.$$

En utilisant à nouveau la relation (1.2), nous obtenons

$$F_{n+2}(X_0, \ldots, X_{n+2}) = X_0 + \frac{1}{F_{n+1}\left(X_1, \ldots, X_{n+1}, X_{n+2}\right)}.$$

Conclusion : Par le principe de récurrence, on a pour tout entier $n \geqslant 0$,

$$F_{n+1}(X_0, \ldots, X_{n+1}) = X_0 + \frac{1}{F_n(X_1, \ldots, X_{n+1})}.$$

□

Dans ce qui suit, nous définissons deux suites de polynômes.

— Soit $(P_n)_{n\geqslant 0}$ la suite de polynômes définie par

$$P_0(X_0) = X_0 \quad \text{et} \quad P_1(X_0, X_1) = X_0X_1 + 1, \tag{1.6}$$

et pour tout $n \geqslant 2$,

$$P_n(X_0, \ldots, X_n) = X_nP_{n-1}(X_0, \ldots, X_{n-1}) + P_{n-2}(X_0, \ldots, X_{n-2}). \tag{1.7}$$

— Soit $(Q_n)_{n\geqslant 0}$ la suite de polynômes définie par

$$Q_0(X_0) = 1 \quad \text{et} \quad Q_1(X_0, X_1) = X_1, \tag{1.8}$$

et pour tout $n \geqslant 2$,

$$Q_n(X_0, \ldots, X_n) = X_nQ_{n-1}(X_0, \ldots, X_{n-1}) + Q_{n-2}(X_0, \ldots, X_{n-2}). \tag{1.9}$$

Proposition 1.2. *Pour tout $n \geqslant 1$, $Q_n(X_0, X_1, \ldots, X_n) = P_{n-1}(X_1, \ldots, X_n)$.*

Démonstration. La preuve se fera par récurrence.

— En utilisant les relations (1.6), (1.8) et (1.9), on vérifie facilement que :

$$Q_1(X_0, X_1) = P_0(X_1) \quad \text{et} \quad Q_2(X_0, X_1, X_2) = P_1(X_1, X_2).$$

— Fixons $n \geqslant 2$. Supposons que pour tout entier k, $1 \leqslant k \leqslant n$,

$$Q_k(X_0, X_1, \ldots, X_k) = P_{k-1}(X_1, \ldots, X_k),$$

et montrons que

$$Q_{n+1}(X_0, X_1, \ldots, X_{n+1}) = P_n(X_1, \ldots, X_{n+1}).$$

Comme $n \geqslant 2$, alors d'après la relation de récurrence (1.9),

$$Q_{n+1}(X_0, X_1, \ldots, X_{n+1}) = X_{n+1}Q_n(X_0, X_1, \ldots, X_n) + Q_{n-1}(X_0, \ldots, X_{n-1}).$$

L'hypothèse de récurrence nous permet de déduire que

$$Q_{n+1}(X_0, X_1, \ldots, X_{n+1}) = X_{n+1}P_{n-1}(X_1, \ldots, X_n) + P_{n-2}(X_1, \ldots, X_{n-1}).$$

Donc en utilisant la relation de récurrence (1.7), nous obtenons

$$Q_{n+1}(X_0, X_1, \ldots, X_{n+1}) = P_n(X_1, \ldots, X_{n+1}).$$

Conclusion : Ainsi, par le principe de récurrence, pour tout entier $n \geqslant 1$, nous avons $Q_n(X_0, X_1, \ldots, X_n) = P_{n-1}(X_1, \ldots, X_n)$. □

Proposition 1.3. *Pour tout $n \geqslant 0$, les coefficients des polynômes P_n et Q_n, définis précédemment, sont des entiers naturels.*

Démonstration. Commençons par le polynôme P_n. Pour cela, nous allons utiliser le raisonnement par récurrence. Pour tout $n \geqslant 0$, notons $A(n)$ l'assertion suivante : les coefficients du polynôme P_n sont des entiers naturels.

- Il est clair que les polynômes P_0 et P_1 donnés par la relation (1.6) sont à coefficients entiers naturels. Ainsi, $A(0)$ et $A(1)$ sont vérifiées.
- Fixons $n \geqslant 1$, supposons que $A(k)$ est vraie pour tout k, $0 \leqslant k \leqslant n$, et montrons que $A(n+1)$ est vraie. En utilisant la relation de récurrence (1.7), nous obtenons ce qui suit :

  $$P_{n+1} = X_{n+1}P_n + P_{n-1}. \tag{1.10}$$

  Comme nous avons supposé que P_n et P_{n-1} ont leurs coefficients dans $\mathbb{N}$, alors (1.10) entraîne que les coefficients du polynôme P_{n+1} sont des entiers naturels.

Conclusion : Par le principe de récurrence, $A(n)$ est vraie pour tout entier $n \geqslant 0$.
Passons maintenant au polynôme Q_n. Il clair que le polynôme Q_0 donné par la relation (1.8) est à coefficients dans $\mathbb{N}$. Il nous reste donc à montrer que pour tout entier $n \geqslant 1$, Q_n est à coefficients dans $\mathbb{N}$. Cela découle de la proposition 1.2 et du fait que le polynôme P_n est à coefficients dans $\mathbb{N}$. □

Proposition 1.4. *Pour tout entier $n \geqslant 0$, $Q_n(X_0, \ldots, X_n) \neq 0$.*

Démonstration. Procédons par récurrence.

- La relation (1.8) montre que $Q_0(X_0), Q_1(X_0, X_1) \neq 0$.
- Fixons $n \geqslant 1$. Supposons que pour tout entier k, $0 \leqslant k \leqslant n$, $Q_k(X_0, \ldots, X_k) \neq 0$, et montrons que $Q_{n+1}(X_0, \ldots, X_n, X_{n+1}) \neq 0$. En utilisant la relation (1.9), nous obtenons ce qui suit :

  $$Q_{n+1}(X_0, \ldots, X_n, X_{n+1}) = X_{n+1}Q_n(X_0, \ldots, X_n) + Q_{n-1}(X_0, \ldots, X_{n-1}).$$

  $Q_{n+1}(X_0, \ldots, X_n, X_{n+1})$ étant un polynôme en X_{n+1} à coefficients dans l'anneau $\mathbb{Z}[X_0, \ldots, X_n]$, dont les coefficients sont non nuls d'après l'hypothèse de récurrence. Ce qui ne permet de déduire que $Q_{n+1}(X_0, \ldots, X_n, X_{n+1}) \neq 0$.

□

Le théorème suivant nous donne la relation entre la fraction rationnelle F_n et les polynômes P_n et Q_n.

Théorème 1.5. *Pour tout entier $n \geqslant 0$,*

$$F_n\left(X_0, \ldots, X_n\right) = \frac{P_n\left(X_0, \ldots, X_n\right)}{Q_n\left(X_0, \ldots, X_n\right)}.$$

Démonstration. Nous allons procéder par récurrence.

— En utilisant les relations (1.1), (1.4), (1.6) et (1.8), on obtient :

$$F_0(X_0) = \frac{P_0(X_0)}{Q_0(X_0)} \text{ et } F_1(X_0, X_1) = \frac{P_1(X_0, X_1)}{Q_1(X_0, X_1)}.$$

— En utilisant les relations de récurrence (1.7) et (1.9) on obtient

$$P_2(X_0, X_1, X_2) = X_2(X_0X_1 + 1) + X_0 \text{ et } Q_2(X_0, X_1, X_2) = X_2X_1 + 1.$$

Ainsi, par la relation (1.5), $F_2(X_0, X_1, X_2) = \frac{P_2(X_0,X_1,X_2)}{Q_2(X_0,X_1,X_2)}$.

— Fixons $n \geqslant 2$. Supposons que pour tout entier k, $0 \leqslant k \leqslant n$,

$$F_k(X_0, \ldots, X_k) = \frac{P_k(X_0, \ldots, X_k)}{Q_k(X_0, \ldots, X_k)} \tag{1.11}$$

et montrons que

$$F_{n+1}(X_0, \ldots, X_{n-1}, X_n, X_{n+1}) = \frac{P_{n+1}(X_0, \ldots, X_{n-1}, X_n, X_{n+1})}{Q_{n+1}(X_0, \ldots, X_{n-1}, X_n, X_{n+1})}.$$

Nous avons par la relation (1.2),

$$F_{n+1}\left(X_0, \ldots, X_{n-1}, X_n, X_{n+1}\right) = F_n\left(X_0, \ldots, X_{n-1}, X_n + \frac{1}{X_{n+1}}\right).$$

Donc, en utilisant l'hypothèse de récurrence (1.11), et les relations de récurrences (1.7) et (1.9), on obtient :

$$\begin{aligned} F_{n+1}\left(X_0, \ldots, X_{n-1}, X_n, X_{n+1}\right) &= \frac{\left(X_n + \frac{1}{X_{n+1}}\right) P_{n-1}\left(X_0, \ldots, X_{n-1}\right) + P_{n-2}\left(X_0, \ldots, X_{n-2}\right)}{\left(X_n + \frac{1}{X_{n+1}}\right) Q_{n-1}\left(X_0, \ldots, X_{n-1}\right) + Q_{n-2}\left(X_0, \ldots, X_{n-2}\right)}. \\ &= \frac{X_{n+1}\left(X_nP_{n-1} + P_{n-2}\right) + P_{n-1}}{X_{n+1}\left(X_nQ_{n-1} + Q_{n-2}\right) + Q_{n-1}}. \end{aligned}$$

En utilisant à nouveau les relations de récurrence (1.7) et (1.9), nous obtenons ce qui suit :

$$\begin{aligned} F_{n+1}\left(X_0, \ldots, X_{n+1}\right) &= \frac{X_{n+1}P_n\left(X_0, \ldots, X_n\right) + P_{n-1}\left(X_0, \ldots, X_{n-1}\right)}{X_{n+1}Q_n\left(X_0, \ldots, X_n\right) + Q_{n-1}\left(X_0, \ldots, X_{n-1}\right)} \\ &= \frac{P_{n+1}\left(X_0, \ldots, X_{n+1}\right)}{Q_{n+1}\left(X_0, \ldots, X_{n+1}\right)}. \end{aligned}$$

Ce qui termine la preuve. □

Théorème 1.6. *Pour tout $n \in \mathbb{N}^*$,*

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}.$$

Démonstration. Procédons par récurrence. L'égalité est clairement vérifiée pour $n = 1$. Fixons $n \geqslant 1$. Supposons que $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}$, alors d'après les relations (1.7) et (1.9)

$$\begin{aligned} P_{n+1}Q_n - Q_{n+1}P_n &= (X_{n+1}P_n + P_{n-1})Q_n - (X_{n+1}Q_n + Q_{n-1})P_n \\ &= -\left(P_nQ_{n-1} - Q_nP_{n-1}\right). \end{aligned}$$

L'hypothèse de récurrence permet de déduire que $P_{n+1}Q_n - Q_{n+1}P_n = (-1)^{n+2}$. □

1.2 Développement en fraction continue d'un nombre réel

Lemme 1.7. *Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'entiers tels que pour tout $n \in \mathbb{N}^*$, $a_n \geqslant 1$. Alors pour tout $n \in \mathbb{N}$*

1. $Q_n(a_0, \ldots, a_n) \in \mathbb{N}^*$.
2. *$F_n(a_0, \ldots, a_n)$ est un nombre rationnel.*

Démonstration.

1. Pour $n = 0$, l'utilisation de la relation (1.8) nous donne $Q_0(a_0) = 1 \in \mathbb{N}^*$. Supposons maintenant que $n \geqslant 1$, la proposition 1.2 nous affirme que dans ce cas,

   $$Q_n(a_0, \ldots, a_n) = P_{n-1}(a_1, \ldots, a_n).$$

   Comme pour tout $1 \leqslant i \leqslant n$, $a_i \in \mathbb{N}^*$, et pour tout $n \geqslant 1$, les coefficients de P_{n-1} sont d'après la proposition 1.3 dans $\mathbb{N}$, alors $Q_n(a_0, \ldots, a_n) \in \mathbb{N}$. On conclut que pour tout $n \geqslant 0$, $Q_n(a_0, \ldots, a_n) \in \mathbb{N}$.
   Il nous reste donc à montrer que pour tout $n \geqslant 0$, $Q_n(a_0, \ldots, a_n) \neq 0$. Pour ce faire nous allons raisonner par récurrence.
   — En utilisant la relation (1.8), on obtient $Q_0(a_0) = 1 \in \mathbb{N}^*$ et $Q_1(a_0, a_1) = a_1$. Comme par hypothèse $a_1 \in \mathbb{N}^*$, alors $Q_1(a_0, a_1) \in \mathbb{N}^*$.
   — Fixons $n \geqslant 1$, supposons que pour tout entier k, $0 \leqslant k \leqslant n$, $Q_k(a_0, \ldots, a_k) \neq 0$, et montrons que $Q_{n+1}(a_0, \ldots, a_n, a_{n+1}) \neq 0$.
   Comme $n \geqslant 1$, alors en utilisant la relation de récurrence (1.9), on obtient :

   $$Q_{n+1}(a_0, \ldots, a_n, a_{n+1}) = a_{n+1}Q_n(a_0, \ldots, a_n) + Q_{n-1}(a_0, \ldots, a_{n-1}).$$

   Puisque $n \geqslant 1$, alors a_{n+1} est par hypothèse un entier strictement positif. En utilisant l'hypothèse de récurrence on peut déduire que $Q_{n+1}(a_0, \ldots, a_n) \neq 0$.
   Conclusion : Par le principe de récurrence, pour tout entier $n \geqslant 1$, $Q_n(a_0, \ldots, a_n) \in \mathbb{N}^*$.

2. Passons à la seconde assertion. Comme pour tout $n \geqslant 0$, $Q_n(a_0, \ldots, a_n) \in \mathbb{N}^*$, alors en utilisant le théorème 1.5, nous obtenons ce qui suit :

$$F_n(a_0, \ldots, a_n) = \frac{P_n(a_0, \ldots, a_n)}{Q_n(a_0, \ldots, a_n)}.$$

Le polynôme P_n est d'après la proposition 1.3 à coefficients dans $\mathbb{N}$, donc comme par hypothèse pour tout $0 \leqslant i \leqslant n$, $a_i \in \mathbb{Z}$, alors $P_n(a_0, \ldots, a_n) \in \mathbb{Z}$. Par conséquent, $F_n(a_0, \ldots, a_n)$ est un nombre rationnel.

□

Définition 1.8. *Soit x un nombre réel. On dit que x admet un développement en fraction continue fini s'il existe $n \in \mathbb{N}$ et des entiers $a_0, a_1 \ldots, a_n$, tels que pour tout $k \in [\![1, n]\!]$, $a_k \geqslant 1$ et $x = F_n(a_0, \ldots, a_n)$.*

Dans ce qui suit nous allons étudier la convergence de la suite $(F_n(a_0, \ldots, a_n))_{n\geqslant 0}$, où $(a_k)_{k\in\mathbb{N}}$ est une suite d'entiers tels que pour tout $k \in \mathbb{N}^*$, $a_k \geqslant 1$. D'après le théorème 1.2

$$F_n(a_0, \ldots, a_n) = \frac{P_n(a_0, \ldots, a_n)}{Q_n(a_0, \ldots, a_n)}. \tag{1.12}$$

Posons pour tout $n \in \mathbb{N}$,

$$p_n = P_n(a_0, \ldots, a_n) \text{ et } q_n = Q_n(a_0, \ldots, a_n). \tag{1.13}$$

de sorte que l'on ait :

$$F_n(a_0, \ldots, a_n) = \frac{p_n}{q_n}. \tag{1.14}$$

D'après les relations (1.6), (1.7), (1.8) et (1.9),

$$p_0 = a_0 \quad \text{et} \quad p_1 = a_1 a_0 + 1, \tag{1.15}$$

$$p_n = a_n p_{n-1} + p_{n-2} \quad \text{pour} \quad n \geqslant 2, \tag{1.16}$$

$$q_0 = 1 \quad \text{et} \quad q_1 = a_1 \tag{1.17}$$

$$q_n = a_n q_{n-1} + q_{n-2} \quad \text{pour} \quad n \geqslant 2 \tag{1.18}$$

Nous avons ainsi obtenu deux suites de nombres $(p_n)_{n\geqslant 0}$ et $(q_n)_{n\geqslant 0}$. Nous allons maintenant donner quelques résultats concernant ces dernières. Parmi ces résultats, certains nous aideront à montrer que la suite $(F_n(a_0, \ldots, a_n))_{n\geqslant 0}$ est convergente.

Lemme 1.9. *Soit n un entier naturel.*

- *Pour tout $n \geqslant 1$, $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$.*
- *Pour tout $n \geqslant 0$, $p_{n+2} q_n - p_n q_{n+2} = (-1)^n a_{n+2}$.*
- *Pour tout $n \geqslant 0$, $\dfrac{p_{2n+1}}{q_{2n+1}} - \dfrac{p_{2n}}{q_{2n}} = \dfrac{1}{q_{2n} q_{2n+1}}$.*

Démonstration.

1. Soit $n \in \mathbb{N}^*$. On a par (1.13),

$$p_n q_{n-1} - q_n p_{n-1} = P_n(a_0, \ldots, a_n) Q_{n-1}(a_0, \ldots, a_{n-1}) - Q_n(a_0, \ldots, a_n) P_{n-1}(a_0, \ldots, a_{n-1}).$$

   Comme $n \geqslant 1$, alors d'après le théorème 1.6,

$$p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}. \tag{1.19}$$

2. Passons à la seconde assertion. Soit $n \geqslant 0$, donc $n+2 \geqslant 2$. Ce qui nous permet d'utiliser les relations (1.16) et (1.18), celles-ci nous donnent :

$$\begin{aligned} p_{n+2} q_n - p_n q_{n+2} &= (a_{n+2} p_{n+1} + p_n)\, q_n - p_n\, (a_{n+2} q_{n+1} + q_n) \\ &= a_{n+2}\, (p_{n+1} q_n - p_n q_{n+1})\,. \end{aligned}$$

   En utilisant la relation (1.19), nous trouvons que $(p_{n+1} q_n - p_n q_{n+1}) = (-1)^{n+2} = (-1)^n$. Par conséquent,

$$p_{n+2} q_n - p_n q_{n+2} = (-1)^n\, a_{n+2}.$$

3. Prouvons la dernière assertion. Soit $n \in \mathbb{N}$,

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{p_{2n+1} q_{2n} - p_{2n} q_{2n+1}}{q_{2n+1} q_{2n}}.$$

   En utilisant (1.19), on obtient :

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n} q_{2n+1}}.$$

□

Corollaire 1.10. *Pour tout entier naturel n, les entiers p_n et q_n sont premiers entre eux.*

Démonstration. D'après les relations (1.15) et (1.17), $p_0 = a_0$ et $q_0 = 1$, avec $a_0 \in \mathbb{Z}$. Il est donc clair que p_0 et q_0 sont premiers entre eux. Supposons maintenant que $n \in \mathbb{N}^*$. Soit d un diviseur de p_n et de q_n. Alors d divise $p_n q_{n-1} - q_n p_{n-1}$, qui, d'après le lemme 1.9, est égal à ± 1. Par conséquent, $d = \pm 1$. Ce qui signifie que p_n et q_n sont premiers entre eux. □

Proposition 1.11. *Si $a_0 \geqslant 1$, alors la suite $(p_n)_{n \geqslant 0}$ est une suite d'entiers strictement positifs, et strictement croissante.*

Démonstration. Commençons par montrer que pour tout entier $n \geqslant 0$, $p_n \in \mathbb{N}^*$.

— D'après la relation (1.15), $p_0 = a_0$. Donc, comme par hypothèse $a_0 \geqslant 1$, alors $p_0 \in \mathbb{N}^*$. Selon la même relation, $p_1 = a_0 a_1 + 1$. Comme $a_0, a_1 \geqslant 1$, alors $a_0 a_1 + 1 \geqslant 2$. Par conséquent, $p_1 \in \mathbb{N}^*$.

— Fixons $n \geqslant 1$. Supposons que pour tout entier k, $0 \leqslant k \leqslant n$, $p_k \in \mathbb{N}^*$, montrons que $p_{n+1} \in \mathbb{N}^*$. D'après la relation (1.16),

$$p_{n+1} = a_{n+1}p_n + p_{n-1}.$$

Comme $a_{n+1} \geqslant 1$, alors l'hypothèse de récurrence nous permet de déduire que $p_{n+1} \in \mathbb{N}^*$.

Conclusion : Par le principe de récurrence, on a pour tout entier $n \geqslant 0$, $p_n \in \mathbb{N}^*$.
Pour finir, montrons que la suite $(p_n)_{n\geqslant 0}$ est strictement croissante. Comme $a_0, a_1 \geqslant 1$, alors

$$a_0a_1 + 1 \geqslant a_0 + 1 > a_0.$$

Par conséquent, en utilisant la relation (1.15), nous obtenons $p_1 > p_0$. Soit $n \geqslant 1$, montrons que $p_{n+1} > p_n$. En utilisant la relation (1.16), nous obtenons

$$p_{n+1} - p_n = (a_{n+1} - 1)p_n + p_{n-1}.$$

Comme $a_{n+1} \geqslant 1$, alors $a_{n+1} - 1 \geqslant 0$. Et puisque la suite $(p_n)_{n\geqslant 0}$ est une suite d'entiers strictement positifs, alors $(a_{n+1}-1)p_n+p_{n-1} \geqslant p_{n-1} > 0$. Par conséquent, $p_{n+1}-p_n > 0$. □

Lemme 1.12. *Pour tout entier $n \geqslant 0$, $q_n \geqslant n$.*

Démonstration. Nous allons raisonner par récurrence.

— Nous avons par la relation (1.17), $q_0 = 1$ et $q_1 = a_1$, avec $a_1 \geqslant 1$. Par conséquent, $q_0 \geqslant 0$ et $q_1 \geqslant 1$.

— Fixons $n \geqslant 1$. Supposons que pour tout entier $0 \leqslant k \leqslant n$, $q_k \geqslant k$ et montrons que $q_{n+1} \geqslant n + 1$. Comme $n + 1 \geqslant 2$, alors en utilisant la relation (1.18) on obtient :

$$q_{n+1} = a_{n+1}q_n + q_{n-1}.$$

Nous avons d'après le lemme 1.7 que $Q_{n-1}(a_0, \ldots, a_{n-1}) \in \mathbb{N}^*$. Donc par (1.13), $q_{n-1} \geqslant 1$. Et comme $a_{n+1} \geqslant 1$, alors

$$q_{n+1} \geqslant q_n + 1.$$

L'hypothèse de récurrence nous permet de déduire que

$$q_{n+1} \geqslant n + 1.$$

Conclusion : Pour tout $n \geqslant 0$, $q_n \geqslant n$. □

Proposition 1.13. *La suite $(q_n)_{n\geqslant 0}$ est une suite d'entiers naturels croissante, et strictement croissante à partir de $n = 1$. De plus, $\lim\limits_{n\to+\infty} q_n = +\infty$.*

Démonstration. Nous avons par la relation (1.17), $q_0 = 1$ et $q_1 = a_1$, où $a_1 \geqslant 1$. Par conséquent, $q_0 \leqslant q_1$.

Soit $n \geqslant 1$, montrons que $q_{n+1} > q_n$. Puisque $n+1 \geqslant 2$, alors en utilisant la relation (1.18), nous obtenons $q_{n+1} = a_{n+1}q_n + q_{n-1}$. Par suite,

$$q_{n+1} - q_n = q_n\left(a_{n+1} - 1\right) + q_{n-1}.$$

Comme $a_{n+1} \geqslant 1$, $q_{n-1} \geqslant 1$ et $q_n \geqslant 1$ alors

$$q_{n+1} - q_n \geqslant 1.$$

Pour finir, nous avons par le lemme 1.12, $q_n \geqslant n$, d'où $\lim\limits_{n\to+\infty} q_n = +\infty$. □

Lemme 1.14. *La suite* $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ *est strictement croissante et la suite* $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ *est strictement décroissante.*

Démonstration. Soit n un entier naturel.

$$\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} = \frac{p_{n+2}q_n - p_nq_{n+2}}{q_nq_{n+2}}.$$

Grâce à la seconde assertion du lemme 1.9, nous obtenons :

$$\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} = \frac{(-1)^n a_{n+2}}{q_nq_{n+2}}.$$

Comme $a_{n+2} \geqslant 1$, alors

$$\begin{cases} \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} > 0 \text{ si } n \text{ est pair} \\ \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} < 0 \text{ si } n \text{ est impair.} \end{cases}$$

Cela signifie que la suite $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ est strictement croissante, et la suite $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ est strictement décroissante. □

Lemme 1.15. *Les suites* $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ *et* $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ *sont adjacentes.*

Démonstration. Soit $n \in \mathbb{N}^*$, on a d'après le lemme 1.9,

$$\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{1}{q_{2n}q_{2n+1}}.$$

Puisque, d'après le lemme 1.13, $\lim\limits_{n\to+\infty} q_n = +\infty$, alors

$$\lim_{n\to+\infty}\left(\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}}\right) = 0.$$

Comme en vertu du lemme 1.14, la suite $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ est strictement croissante et la suite $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ est strictement décroissante, alors ces dernières sont adjacentes. □

Maintenant nous avons les outils pour montrer que la suite $(F_n(a_0, \ldots, a_n))_{n\geqslant 0}$ est convergente.

Proposition 1.16. *Soit $(a_n)_{n\geqslant 0}$ une suite de nombres entiers telle que pour tout $n \geqslant 1$, $a_n \geqslant 1$. Alors la suite $(F_n(a_0, \ldots, a_n))_{n\geqslant 0}$ est convergente.*

Démonstration. En utilisant (1.13), (1.12) devient comme suit :

$$F_n(a_0, \ldots, a_n) = \frac{p_n}{q_n}.$$

Montrons donc que la suite $\left(\frac{p_n}{q_n}\right)_{n\geqslant 0}$ est convergente. Comme les sous-suites $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ et $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ sont en vertu du lemme 1.15 adjacentes, alors elles convergent vers une limite commune ℓ. Par conséquent, la suite $\left(\frac{p_n}{q_n}\right)_{n\geqslant 0}$ converge également vers ℓ. □

Cette proposition rend légitime la définition suivante :

Définition 1.17. *Soit x un nombre réel. On dit que x admet un développement en fraction continue infini s'il existe une suite d'entiers $(a_n)_{n\geqslant 0}$, avec $a_n \geqslant 1$, pour tout $n \geqslant 1$, vérifiant*

$$x = \lim_{n\to+\infty} F_n(a_0, \ldots, a_n).$$

Proposition 1.18. *Si un nombre réel x admet un développement en fraction continue infini alors x est irrationel.*

Démonstration. Procédons par l'absurde. Supposons qu'il existe $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x = \frac{a}{b}$ et que x admet un développement en fraction continue infini. Donc il existe une suite d'entiers $(a_n)_{n\geqslant 0}$, tel que, pour tout $n \geqslant 1$, $a_n \geqslant 1$, vérifiant

$$x = \lim_{n\to+\infty} F_n(a_0, \ldots, a_n).$$

En utilisant (1.14), nous obtenons $\frac{a}{b} = \lim_{n\to+\infty} \frac{p_n}{q_n}$. Par conséquent, les sous-suites $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ et $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ convergent vers x. Puisque, d'après le lemme 1.14, $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ est strictement croissante et $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ est strictement décroissante, alors pour tout $n \geqslant 0$,

$$\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+2}}{q_{2n+2}} \leqslant \frac{a}{b} \leqslant \frac{p_{2n+3}}{q_{2n+3}} < \frac{p_{2n+1}}{q_{2n+1}}.$$

Par suite,

$$0 < \frac{a}{b} - \frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}}.$$

Donc, d'après la troisième assertion du lemme 1.9,

$$0 < \frac{a}{b} - \frac{p_{2n}}{q_{2n}} < \frac{1}{q_{2n}q_{2n+1}}.$$

D'où

$$0 < aq_{2n} - bp_{2n} < \frac{b}{q_{2n+1}}.$$

Puisque la suite $(q_n)_{n\geqslant 0}$ tend vers $+\infty$, alors il existe nécessairement un entier $k \geqslant 1$, tel que $q_{2k+1} > b$, et donc

$$0 < aq_{2k} - bp_{2k} < 1.$$

Ce qui contredit le fait que $aq_{2k} - bp_{2k}$ est un entier. □

Proposition 1.19. *Soit $x \in \mathbb{R}$. Le réel x est un nombre rationnel si et seulement s'il admet un développement en fraction continue fini.*

Démonstration. Soit $x \in \mathbb{Q}$, il existe alors $(r_0, r_1) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $x = \frac{r_0}{r_1}$. En appliquant l'algorithme d'Euclide sur la paire (r_0, r_1), on obtient deux suites d'entiers finies $(a_k)_{0\leqslant k\leqslant n}$ et $(r_k)_{0\leqslant k\leqslant n+2}$, tels que pour tout $k \in [\![1, n]\!]$, $a_k \geqslant 1$, et pour tout $k \in [\![0, n]\!]$, on a :

$$r_k = r_{k+1}a_k + r_{k+2}, \tag{1.20}$$

avec $0 < r_{k+2} < r_{k+1}$, pour tout $k \in [\![0, n-1]\!]$, et $r_{n+1} = \text{pgcd}(r_0, r_1)$ et $r_{n+2} = 0$.

— Si $n = 0$, alors $x = \frac{r_0}{r_1} = a_0 = F_0(a_0)$. Par conséquent, x admet un développement en fraction continue fini.

— Supposons que $n \geqslant 1$. On se propose de montrer que pour tout $k \in [\![1, n]\!]$, on a :

$$x = F_k\left(a_0, \ldots, a_{k-1}, \frac{r_k}{r_{k+1}}\right). \tag{1.21}$$

— Pour $k = 1$, on a $r_0 = r_1a_0 + r_2$ avec $r_2 > 0$. Par conséquent,

$$x = \frac{r_0}{r_1} = a_0 + \frac{1}{\frac{r_1}{r_2}} = F_1(a_0, \frac{1}{r_2}).$$

— Soit $k \in [\![1, n-1]\!]$. On suppose que $x = F_k\left(a_0, \ldots, a_{k-1}, \frac{r_k}{r_{k+1}}\right)$, et montrons que

$$x = F_{k+1}\left(a_0, \ldots, a_k, \frac{r_{k+1}}{r_{k+2}}\right).$$

Comme $k \in [\![1, n-1]\!]$, alors $k + 2 \leqslant n + 1$, et donc $r_{k+2} \neq 0$. D'où, par (1.20),

$$\frac{r_k}{r_{k+1}} = a_k + \frac{1}{\frac{r_{k+1}}{r_{k+2}}}.$$

Par conséquent,

$$x = F_k\left(a_0, \ldots, a_{k-1}, a_k + \frac{1}{\frac{r_{k+1}}{r_{k+2}}}\right).$$

Grâce à la relation de récurrence (1.2), on obtient

$$F_{k+1}\left(a_0, \ldots, a_k, \frac{r_{k+1}}{r_{k+2}}\right).$$

Dans le cas particulier $k = n$, la relation (1.21) donne

$$x = F_n\left(a_0, \ldots, a_{n-1}, \frac{r_n}{r_{n+1}}\right). \tag{1.22}$$

D'après (1.20), $\frac{r_n}{r_{n+1}} = a_n + \frac{r_{n+2}}{r_{n+1}}$. Mais comme $r_{n+1} = \text{pgcd}(r_0, r_1)$, alors $r_{n+2} = 0$. Par conséquent, $\frac{r_n}{r_{n+1}} = a_n$. Ce qui nous permet de réécrire (1.22), comme suit :

$$x = F_n\left(a_0, \ldots, a_{n-1}, a_n\right).$$

On conclut que pour tout $n \in \mathbb{N}^*$, x admet un développement en fraction continue fini.

Réciproquement, supposons que le réel x admet un développement en fraction continue fini, c'est-à-dire qu'il existe des entiers $a_0, a_1 \ldots, a_n$, tels que pour tout $k \in [\![1, n]\!]$, $a_k \geqslant 1$ et $x = F_n(a_0, \ldots, a_n)$. D'après le lemme 1.7, $F_n(a_0, \ldots, a_n)$ est un nombre rationnel. Ce qui termine la preuve. □

Proposition 1.20. *Soit x un nombre rationnel. Alors x admet deux développements en fraction continue finis.*

Démonstration. Soit $x \in \mathbb{Q}$, il existe d'après la proposition 1.19, $n \in \mathbb{N}$ et des entiers $a_0, a_1 \ldots, a_n$, tels que pour tout $k \in [\![1, n]\!]$, $a_k \geqslant 1$ et

$$x = F_n(a_0, \ldots, a_n).$$

Il est clair que si $x = F_0(a_0)$, alors $x \in \mathbb{Z}$. Et dans ce cas $x = F_1(a_0 - 1, 1)$. On peut supposer donc que $n \geqslant 1$.

$$x = F_n(a_0, \ldots, a_n) = \begin{cases} F_{n-1}(a_0, \ldots, a_{n-1} + 1) & \text{si } a_n = 1 \\ \\ F_{n+1}(a_0, \ldots, a_n - 1, 1) & \text{si } a_n > 1. \end{cases}$$

En effet :

— Supposons que $a_n = 1$. Donc, $x = F_n(a_0, \ldots, a_{n-1}, 1)$. Grâce à la relation (1.2), on obtient :

$$x = F_{n-1}(a_0, \ldots, a_{n-1} + 1).$$

— Supposons que $a_n > 1$. En utilisant à nouveau la relation (1.2), on peut réécrire x comme suit :

$$x = F_{n+1}\left(a_0, \ldots, (a_n - 1), 1\right).$$

Nous remarquons que dans les deux cas, x admet deux développements en fraction continue finis. □

Nous clôturons cette section par prouver que si un nombre irrationnel admet un développement en fraction continue infini, alors ce dernier est unique. Pour ce faire nous aurons

besoin du théorème suivant.

Théorème 1.21. *Soient x un nombre irrationnel, $(a_n)_{n\geqslant 0}$ une suite d'entiers tels que pour tout entier $n \geqslant 1$, $a_n \geqslant 1$ et $x = \lim\limits_{n\to+\infty} F_n(a_0, \ldots, a_n)$. Soit $(x_n)_{n\geqslant 0}$ la suite définie pour tout $n \geqslant 0$ par $x_n = \lim\limits_{k\to+\infty} F_k(a_n, \ldots, a_{n+k})$. Alors pour tout entier $n \geqslant 0$*

1. $x_n = a_n + \frac{1}{x_{n+1}}$.
2. $x_{n+1} > 1$.
3. $a_n = \lfloor x_n \rfloor$.

Démonstration.

1. Commençons par prouver que pour tout entier n, $x_{n+1} \geqslant 1$. D'après le théorème 1.5

$$F_k(a_{n+1}, \ldots, a_{n+k+1}) = \frac{P_k(a_{n+1}, \ldots, a_{n+k+1})}{Q_k(a_{n+1}, \ldots, a_{n+k+1})}.$$

D'après la proposition 1.3, les deux polynômes P_n et Q_n sont à coefficients dans $\mathbb{N}$, comme par hypothèse $a_{n+1}, \ldots, a_{n+k+1}$ sont des entiers strictement positifs, alors il n'est pas difficile d'en déduire que pour tout entier $k \geqslant 0$,

$$P_k(a_{n+1}, \ldots, a_{n+k+1}) \in \mathbb{N}^* \text{ et } Q_k(a_{n+1}, \ldots, a_{n+k+1}) \in \mathbb{N}^*.$$

Par conséquent, pour tout $k \in \mathbb{N}$, $F_k(a_{n+1}, \ldots, a_{n+k+1}) > 0$. Or d'après la proposition 1.1, pour tout $k \geqslant 1$

$$F_k(a_{n+1}, \ldots, a_{n+k+1}) = a_{n+1} + \frac{1}{F_{k-1}(a_{n+2}, \ldots, a_{n+k+1})}.$$

Comme par hypothèse $a_{n+1} \geqslant 1$ alors pour tout $k \geqslant 1$, $F_k(a_{n+1}, \ldots, a_{n+k+1}) > 1$. Donc $\lim\limits_{k\to+\infty} F_k(a_{n+1}, \ldots, a_{n+k+1}) \geqslant 1$. Autrement dit

$$x_{n+1} \geqslant 1, \qquad \text{pour tout } n \geqslant 0. \tag{1.23}$$

2. Montrons que pour tout $n \geqslant 0$, $x_n = a_n + \frac{1}{x_{n+1}}$. Nous avons par hypothèse

$$\begin{aligned} x_n &= \lim_{k\to+\infty} F_k(a_n, \ldots, a_{n+k}) \\ &= \lim_{k\to+\infty} F_{k+1}(a_n, \ldots, a_{n+k+1}). \end{aligned}$$

En utilisant la proposition 1.1, nous obtenons ce qui suit :

$$\begin{aligned} x_n &= \lim_{k\to+\infty} \left(a_n + \frac{1}{F_k(a_{n+1}, \ldots, a_{n+k+1})} \right) \\ &= a_n + \frac{1}{\lim\limits_{k\to+\infty} F_k(a_{n+1}, \ldots, a_{n+k+1})} \\ &= a_n + \frac{1}{x_{n+1}}. \end{aligned}$$

3. Montrons que pour tout entier $n \geqslant 0$, $x_{n+1} > 1$. D'après l'assertion précédente,

$$x_{n+1} = a_{n+1} + \frac{1}{x_{n+2}}.$$

Par conséquent, la relation (1.23) donne $x_{n+1} > a_{n+1}$. Vu que $a_{n+1} \geqslant 1$, il en résulte que $x_{n+1} > 1$.

4. Prouvons la dernière assertion. Comme, d'après l'assertion précédente, pour tout entier $n \geqslant 0$, $x_{n+1} > 1$, alors $0 < \frac{1}{x_{n+1}} < 1$. Par suite, $a_n < a_n + \frac{1}{x_{n+1}} < a_n + 1$. Donc, d'après la première assertion, $a_n < x_n < a_n + 1$. Ce qui signifie que $a_n = \lfloor x_n \rfloor$.

□

Corollaire 1.22. *Soit x un nombre irrationnel. Si x admet un développement en fraction continue infini, alors il est unique.*

Démonstration. Supposons par l'absurde qu'il existe deux suites d'entiers différentes $(a_n)_{n\geqslant 0}$ et $(b_n)_{n\geqslant 0}$ telles que pour tout entier $n \geqslant 1$, $a_n, b_n \geqslant 1$ et

$$x = \lim_{n\to+\infty} F_n(a_0, \ldots, a_n) = \lim_{n\to+\infty} F_n(b_0, \ldots, b_n).$$

Considérons pour tout entier $n \geqslant 0$, les suites $(x_n)_{n\geqslant 0}$ et $(y_n)_{n\geqslant 0}$ définies pour tout entier $n \geqslant 0$ par,

$$x_n = \lim_{k\to+\infty} F_k(a_n, \ldots, a_{n+k}) \text{ et } y_n = \lim_{k\to+\infty} F_k(b_n, \ldots, b_{n+k}).$$

D'après le théorème 1.21, pour tout entier $n \geqslant 0$,

$$x_{n+1} = \frac{1}{x_n - a_n},\ y_{n+1} = \frac{1}{y_n - b_n},\ a_n = \lfloor x_n \rfloor \text{ et } b_n = \lfloor y_n \rfloor. \tag{1.24}$$

Prouvons pour tout entier $n \geqslant 0$, $x_n = y_n$.

— Il est clair que $x_0 = x$ et $y_0 = x$. Donc la relation est vérifiée pour $n = 0$.

— Fixons $n \geqslant 0$. Supposons que $x_n = y_n$ et montrons que $x_{n+1} = y_{n+1}$. Comme $x_n = y_n$, alors $a_n = b_n$. Ainsi, en utilisant la relation (1.24), nous obtenons ce qui suit :

$$x_{n+1} = \frac{1}{y_n - b_n}.$$

En utilisant à nouveau la relation (1.24), nous obtenons $x_{n+1} = y_{n+1}$.

Conclusion : Par le principe de récurrence, pour tout entier $n \geqslant 0$, $x_n = y_n$.
Il en résulte que pour tout entier $n \geqslant 0$, $a_n = b_n$. Ce qui contredit notre hypothèse. Donc, x admet un unique développement en fraction continue. □

1.3 Développement en fraction continue d'un nombre irrationnel

Nous verrons un peu plus loin que si x est un nombre irrationnel, alors il admet un développement en fraction continue infini. La démonstration de ce résultat nécessite d'autres résultats que nous donnerons dans ce qui suit.
Soit x un nombre irrationnel. Considérons les suites $(a_n)_{n\geqslant 0}$ et $(x_n)_{n\geqslant 0}$ définies par $x_0 = x$ et pour tout $n \geqslant 0$

$$a_n = \lfloor x_n \rfloor \text{ et } x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor}. \tag{1.25}$$

La suite $(x_n)_{n\in\mathbb{N}}$ est bien définie. En effet, nous verrons dans la proposition suivante que pour tout $n \in \mathbb{N}$, x_n est irrationnel, ce qui entraîne que $x_n - \lfloor x_n \rfloor \neq 0$.

Proposition 1.23.

1. *La suite $(x_n)_{n\geqslant 0}$ est une suite d'irrationnels, tel que pour tout $n \geqslant 1$, $x_n > 1$.*
2. *La suite $(a_n)_{n\geqslant 0}$ est une suite d'entiers, tel que pour tout $n \geqslant 1$, $a_n \geqslant 1$.*
3. *Pour tout $n \geqslant 0$, $x = F_{n+1}(a_0, \ldots, a_n, x_{n+1})$.*

Démonstration.

1. Nous allons montrer par récurrence que pour tout entier $n \geqslant 0$, $x_n \notin \mathbb{Q}$.
   — Pour $n = 0$, nous avons $x_0 = x$ qui est un nombre irrationnel.
   — Fixons $n \geqslant 0$. Supposons que $x_n \notin \mathbb{Q}$, et montrons que $x_{n+1} \notin \mathbb{Q}$. Comme $x_n \notin \mathbb{Q}$ alors $x_n - \lfloor x_n \rfloor \notin \mathbb{Q}$. Par conséquent $x_{n+1} = \dfrac{1}{x_n - \lfloor x_n \rfloor} \notin \mathbb{Q}$.
   Soit $n \geqslant 1$, montrons que $x_n > 1$. Puisque x_n est irrationnel, alors

   $$0 < x_n - \lfloor x_n \rfloor < 1.$$

   D'où

   $$x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor} > 1.$$

   Cela signifie que pour tout $n \geqslant 1$, $x_n > 1$.

2. Passons à la seconde assertion. Soit $n \geqslant 1$. On a d'après l'assertion précédente $x_n > 1$. Par conséquent $a_n = \lfloor x_n \rfloor \geqslant 1$.

3. Pour finir, montrons la dernière assertion. Pour cela nous allons procéder par récurrence.
   — On a $x_1 = \dfrac{1}{x_0 - a_0}$, donc $x_0 = a_0 + \dfrac{1}{x_1} = F_1(a_0, x_1)$.
   — Fixons $n \geqslant 0$. Supposons que $x = F_{n+1}(a_0, \ldots, a_n, x_{n+1})$, et montrons que

   $$x = F_{n+2}(a_0, \ldots, a_n, a_{n+1}, x_{n+2}).$$

Nous avons par définition de la suite $(x_n)_{n\in\mathbb{N}}$, $x_{n+2} = \frac{1}{x_{n+1}-a_{n+1}}$. D'où

$$x_{n+1} = a_{n+1} + \frac{1}{x_{n+2}}.$$

Par suite,

$$x = F_{n+1}\left(a_0, \ldots, a_n, a_{n+1} + \frac{1}{x_{n+2}}\right).$$

Grâce à la relation de récurrence (1.2), nous obtenons

$$x = F_{n+2}(a_0, \ldots, a_n, a_{n+1}, x_{n+2}).$$

□

Définition 1.24. *Pour tout entier $n \geqslant 0$, $F_n(a_0, \ldots, a_n)$ s'appelle réduite d'ordre n.*

La suite $(a_n)_{n\geqslant 0}$ est d'après la proposition 1.23, une suite d'entiers tel que pour tout $n \geqslant 1$, $a_n \geqslant 1$. Donc, d'après le lemme 1.7, $F_n(a_0, \ldots, a_n)$ est un nombre rationnel. Selon le théorème 1.5,

$$F_n(a_0, \ldots, a_n) = \frac{P_n(a_0, \ldots, a_n)}{Q_n(a_0, \ldots, a_n)}.$$

Posons pour tout $n \in \mathbb{N}$,

$$p_n = P_n(a_0, \ldots, a_n) \text{ et } q_n = Q_n(a_0, \ldots, a_n), \tag{1.26}$$

de sorte que l'on ait :

$$F_n(a_0, \ldots, a_n) = \frac{p_n}{q_n}.$$

D'après les relations (1.6), (1.7), (1.8) et (1.9),

$$p_0 = a_0 \quad \text{et} \quad p_1 = a_1a_0 + 1, \tag{1.27}$$

$$p_n = a_np_{n-1} + p_{n-2}, \quad \text{pour tout } n \geqslant 2, \tag{1.28}$$

$$q_0 = 1 \quad \text{et} \quad q_1 = a_1, \tag{1.29}$$

$$q_n = a_nq_{n-1} + q_{n-2} \quad \text{pour tout } n \geqslant 2. \tag{1.30}$$

Lemme 1.25. *Pour tout entier $n \geqslant 1$, nous avons :*

1. $x = \dfrac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$.
2. $x - \dfrac{p_n}{q_n} = \dfrac{(-1)^n}{q_n(x_{n+1}q_n + q_{n-1})}$.

Démonstration.

1. Soit $n \in \mathbb{N}^*$. D'après la dernière assertion de la proposition 1.23,

$$x = F_{n+1}(a_0, \ldots, a_n, x_{n+1}) = \frac{P_{n+1}\left(a_0, a_1, \ldots, a_n, x_{n+1}\right)}{Q_{n+1}\left(a_0, a_1, \ldots, a_n, x_{n+1}\right)}.$$

   Les relations de récurrences (1.7) et (1.9), nous permettent de réécrire x comme suit :

$$x = \frac{x_{n+1}P_n\left(a_0, \ldots, a_n\right) + P_{n-1}\left(a_0, \ldots, a_{n-1}\right)}{x_{n+1}Q_n\left(a_0, \ldots, a_n\right) + Q_{n-1}\left(a_0, \ldots, a_{n-1}\right)}.$$

   En utilisant les notations données par (1.26), nous obtenons

$$x = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}. \tag{1.31}$$

2. Pour finir, prouvons la seconde assertion. Soit $n \in \mathbb{N}^*$. En utilisant la relation (1.31), nous obtenons :

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{(x_{n+1}p_n + p_{n-1})q_n - p_n(x_{n+1}q_n + q_{n-1})}{q_n(x_{n+1}q_n + q_{n-1})} \\ &= \frac{-\left(p_nq_{n-1} - p_{n-1}q_n\right)}{q_n(x_{n+1}q_n + q_{n-1})}. \end{aligned}$$

   En utilisant l'assertion (1) du lemme 1.9, nous obtenons :

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n\left(x_{n+1}q_n + q_{n-1}\right)}.$$

□

Proposition 1.26.

1. *Pour tout entier* $n \geqslant 0$, $\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$.
2. *La suite* $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ *converge vers* x.
3. *Pour tout* $n \geqslant 0$, $\frac{p_{2n}}{q_{2n}} < x < \frac{p_{2n+1}}{q_{2n+1}}$.
4. *Pour tout entier* $n \geqslant 0$, $q_nx - p_n$ *et* $q_{n+1}x - p_{n+1}$ *sont de signes contraires.*

Démonstration.

1. Commençons par montrer que la formule est vérifiée pour $n = 0$. En utilisant les relations (1.27) et (1.29), nous obtenons

$$\left|x - \frac{p_0}{q_0}\right| = \left|x - a_0\right|,$$

   où, $a_0 = \lfloor x \rfloor$ (voir la relation (1.25)). Comme $0 < x - \lfloor x \rfloor < 1$, alors $\left|x - \frac{p_0}{q_0}\right| < 1$. En

utilisant à nouveau la relation (1.29), nous obtenons :

$$\left|x - \frac{p_0}{q_0}\right| < \frac{1}{q_0^2}.$$

Supposons maintenant que $n \in \mathbb{N}^*$. Nous avons d'après le lemme 1.25,

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n\left(x_{n+1}q_n + q_{n-1}\right)}.$$

Comme, $q_n, q_{n-1} > 0$, et d'après la proposition 1.23, $x_{n+1} > 1$, alors

$$x_{n+1}q_n + q_{n-1} > q_n.$$

Par conséquent

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}. \tag{1.32}$$

2. D'après la proposition 1.13, $\lim\limits_{n\to+\infty} q_n = +\infty$. Par conséquent la relation (1.32) entraîne que

$$\lim_{n\to+\infty} \frac{p_n}{q_n} = x.$$

3. Montrons que $\left(\frac{p_{2n}}{q_{2n}}\right)_{n\geqslant 0}$ est majorée par x. En utilisant les relations (1.27) et (1.29), on obtient

$$\frac{p_0}{q_0} - x = a_0 - x,$$

avec $a_0 = \lfloor x \rfloor$ (voir (1.25)). Comme $x \notin \mathbb{Q}$, alors $x - \lfloor x \rfloor > 0$. Par conséquent,

$$\frac{p_0}{q_0} - x < 0. \tag{1.33}$$

Soit $n \in \mathbb{N}^*$, en utilisant la dernière assertion du lemme 1.25, on obtient

$$\frac{p_{2n}}{q_{2n}} - x = \frac{-1}{q_{2n}\left(x_{2n+1}q_{2n} + q_{2n-1}\right)}.$$

donc,

$$\frac{p_{2n}}{q_{2n}} - x < 0.$$

On déduit de cette inégalité et de l'inégalité (1.33) que pour tout $n \in \mathbb{N}$, $\frac{p_{2n}}{q_{2n}} < x$.
Pour finir, montrons que la suite $\left(\frac{p_{2n+1}}{q_{2n+1}}\right)_{n\geqslant 0}$ est minorée par x. Soit $n \in \mathbb{N}$. En utilisant à nouveau la dernière assertion du lemme 1.25, on obtient,

$$x - \frac{p_{2n+1}}{q_{2n+1}} = \frac{-1}{q_{2n+1}(x_{2n+2}q_{2n+1} + q_{2n})} < 0.$$

Par conséquent, $x < \frac{p_{2n+1}}{q_{2n+1}}$.

4. Soit n un entier naturel,

$$(xq_n - p_n)(xq_{n+1} - p_{n+1}) = q_n q_{n+1}\left(x - \frac{p_n}{q_n}\right)\left(x - \frac{p_{n+1}}{q_{n+1}}\right).$$

Comme $q_n q_{n+1} > 0$, alors le signe de $(xq_n - p_n)(xq_{n+1} - p_{n+1})$ est égal au signe de $\left(x - \frac{p_n}{q_n}\right)\left(x - \frac{p_{n+1}}{q_{n+1}}\right)$. Or d'après l'assertion précédente, selon la parité de n deux cas se présentent. Si n est pair, alors, $x - \frac{p_n}{q_n} > 0$ et $x - \frac{p_{n+1}}{q_{n+1}} < 0$. Alors que si n est impair $x - \frac{p_n}{q_n} < 0$ et $x - \frac{p_{n+1}}{q_{n+1}} > 0$. Conclusion : Pour tout entier $n \geqslant 0$, $q_n x - p_n$ et $q_{n+1}x - p_{n+1}$ sont de signes contraires.

□

1.4 Quelques propriétés du développement en fraction continue

En conclusion de la section précédente, notamment l'assertion (2) de la proposition 1.26, tout nombre réel irrationnel admet un développement en fraction continue infini. La réciproque à ce résultat est assurée par la proposition 1.18. Ce qui nous permet de déduire aisément le théorème suivant.

Théorème 1.27. *Un nombre réel est irrationnel si et seulement s'il admet un développement en fraction continue infini.*

Le résultat suivant, prouvé par Andrien-Marie Legendre en 1798, est d'une grande importance. Il nous sera utile pour l'étude de l'équation de Pell-Fermat (2.1).

Théorème 1.28 (Legendre [13])**.** *Soit x un nombre irrationnel et p et q deux entiers tels que $q > 0$ et*

$$\left|x - \frac{p}{q}\right| < \frac{1}{2q^2},$$

alors $\frac{p}{q}$ est une réduite de x.

La preuve de ce théorème nécessite les résultats suivants. Dans la suite, on considère un nombre réel x irrationnel. On notera $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ la suite des réduites de x.

Lemme 1.29. *Soient $n \in \mathbb{N}$, p et q deux entiers relatifs tels que $1 \leqslant q < q_{n+1}$. Alors, il existe $(u, v) \in \mathbb{Z}^* \times \mathbb{Z}$, tel que :*

$$p = up_n + vp_{n+1} \qquad et \qquad q = uq_n + vq_{n+1}.$$

De plus, si $v \neq 0$, alors u et v sont de signes contraires.

Démonstration. Soit n un entier naturel. Considérons la matrice suivante :

$$A = \begin{pmatrix} p_n & p_{n+1} \\ q_n & q_{n+1} \end{pmatrix}. \tag{1.34}$$

On a, $detA = p_n q_{n+1} - q_n p_{n+1}$. En utilisant la première assertion du lemme 1.9, nous obtenons : $\det A = (-1)^{n+1}$. Donc la matrice A est inversible dans $\mathbb{M}_2(\mathbb{Z})$, d'inverse

$$A^{-1} = (-1)^{n+1} \begin{pmatrix} q_{n+1} & -p_{n+1} \\ -q_n & p_n \end{pmatrix} \in \mathbb{M}_2(\mathbb{Z}).$$

Soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$. Posons

$$\begin{pmatrix} u \\ v \end{pmatrix} = A^{-1} \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} (-1)^{n+1}(q_{n+1}p - p_{n+1}q) \\ (-1)^{n+1}(p_n q - q_n p) \end{pmatrix}.$$

Autrement dit $u = (-1)^{n+1}(q_{n+1}p - p_{n+1}q)$ et $v = (-1)^{n+1}(p_n q - q_n p)$, qui sont clairement des entiers. Donc,

$$\begin{pmatrix} p \\ q \end{pmatrix} = A \begin{pmatrix} u \\ v \end{pmatrix}.$$

En utilisant (1.34), nous obtenons

$$\begin{aligned} p &= up_n + vp_{n+1} \\ q &= uq_n + vq_{n+1}. \end{aligned} \tag{1.35}$$

Montrons maintenant que $u \neq 0$. Supposons que $u = 0$, alors (1.35) devient comme suit : $q = vq_{n+1}$. Ce qui contredit l'hypothèse $1 \leqslant q < q_{n+1}$. Par conséquent, $u \neq 0$.
Pour finir, montrons que si $v \neq 0$, alors u et v sont de signes contraires. Comme $q < q_{n+1}$, alors en utilisant (1.35), on obtient l'inégalité suivante : $1 \leqslant uq_n + vq_{n+1} < q_{n+1}$. Par suite,

$$1 - vq_{n+1} \leqslant uq_n < (1 - v)\, q_{n+1}. \tag{1.36}$$

Comme v est un entier non nul, alors deux cas sont possible.

- **Cas 1** : $v \geqslant 1$.
  Dans ce cas $1 - v \leqslant 0$. Comme $q_{n+1} > 0$, alors $(1 - v)\, q_{n+1} \leqslant 0$. Ainsi, en utilisant l'inégalité (1.36) on obtient que $uq_n < 0$. Et puisque $q_n > 0$, alors $u < 0$.
- **Cas 2** : $v \leqslant -1$.
  Dans ce cas $1 - vq_{n+1} > 0$. Ainsi, en utilisant l'inégalité (1.36) on obtient que $uq_n > 0$. Et puisque $q_n > 0$, alors $u > 0$.

Conclusion : dans les deux cas, u et v sont de signes contraires. □

Proposition 1.30. *Soient $n \in \mathbb{N}$ et p et q deux entiers rationnels tels que $1 \leqslant q < q_{n+1}$. Alors*

$$|qx - p| \geqslant |q_n x - p_n|.$$

Démonstration. Soient p et q deux entiers. Il existe d'après le lemme 1.29, $(u, v) \in \mathbb{Z}^* \times \mathbb{Z}$,

tels que

$$p = up_n + vp_{n+1} \tag{1.37}$$

$$q = uq_n + vq_{n+1}. \tag{1.38}$$

Comme v est un entier, alors deux cas se présentent.

— **Cas 1** : $v = 0$.
D'après, (1.37) et (1.38), on a

$$|qx - p| = |u| \, |q_n x - p_n| \, .$$

Puisque $u \in \mathbb{Z}^*$, alors $|u| \geqslant 1$. Par conséquent, $|qx - p| \geqslant |q_n x - p_n|$.

— **Cas 2** : $v \neq 0$. En utilisant (1.37) et (1.38), on obtient :

$$\begin{aligned} |qx - p| &= |(uq_n + vq_{n+1})\, x - (up_n + vp_{n+1})| \\ &= |u\,(q_n x - p_n) + v\,(q_{n+1}x - p_{n+1})| \, . \end{aligned}$$

Comme, d'après le lemme 1.29, u et v sont de signes contraires, et $q_n x - p_n$, $q_{n+1}x - p_{n+1}$ le sont également d'après l'assertion (4) du lemme 1.26, alors $u\,(q_n x - p_n)$ et $v\,(q_{n+1}x - p_{n+1})$ sont de même signe. Par conséquent,

$$|qx - p| = |u| \, |q_n x - p_n| + |v| \, |q_{n+1}x - p_{n+1}| \, .$$

Par suite,

$$|qx - p| \geqslant |u| \, |q_n x - p_n| \, .$$

Puisque $|u| \geqslant 1$, alors

$$|u| \, |q_n x - p_n| \geqslant |q_n x - p_n| \, .$$

Par conséquent,

$$|qx - p| \geqslant |q_n x - p_n| \, .$$

Ainsi s'achève cette preuve. □

Nous pouvons à présent donner la preuve du théorème 1.28.

Démonstration du théorème 1.28. Considérons l'ensemble $E = \{k \in \mathbb{N} \mid q_k \leqslant q\}$. Comme $q \geqslant 1$ alors $E \neq \emptyset$. D'après la proposition 1.13, la suite $(q_k)_{k \geqslant 1}$ est une suite d'entiers qui tend vers $+\infty$. Par conséquent l'ensemble E est fini. Posons alors

$$n = \max\{k \in \mathbb{N} \mid q_k \leqslant q\}.$$

L'entier n vérifie donc

$$q_n \leqslant q < q_{n+1}. \tag{1.39}$$

Nous avons,

$$\begin{aligned}\left|\frac{p}{q}-\frac{p_n}{q_n}\right| &= \left|\left(\frac{p}{q}-x\right)+\left(x-\frac{p_n}{q_n}\right)\right| \\ &\leqslant \left|x-\frac{p}{q}\right|+\left|x-\frac{p_n}{q_n}\right| \\ &= \left|\frac{qx-p}{q}\right|+\left|\frac{q_nx-p_n}{q_n}\right|.\end{aligned}$$

Comme $q, q_n \geqslant 1$, alors

$$\left|\frac{p}{q}-\frac{p_n}{q_n}\right| \leqslant \frac{1}{q}\left|qx-p\right|+\frac{1}{q_n}\left|q_nx-p_n\right|. \tag{1.40}$$

Comme par la relation (1.39), $1 \leqslant q < q_{n+1}$, alors, d'après la proposition 1.30

$$\left|q_nx-p_n\right| \leqslant \left|qx-p\right|.$$

Par conséquent,

$$\frac{1}{q_n}\left|q_nx-p_n\right|+\frac{1}{q}\left|qx-p\right| \leqslant \left(\frac{1}{q_n}+\frac{1}{q}\right)\left|qx-p\right|.$$

Compte tenu de cette inégalité et de l'inégalité (1.40), nous obtenons :

$$\left|\frac{p}{q}-\frac{p_n}{q_n}\right| \leqslant \left(\frac{1}{q_n}+\frac{1}{q}\right)\left|qx-p\right|. \tag{1.41}$$

Comme par hypothèse $\left|x-\frac{p}{q}\right| < \frac{1}{2q^2}$, alors

$$\left|qx-p\right| < \frac{1}{2q}. \tag{1.42}$$

Et puisque nous avons par (1.39), $0 < q_n \leqslant q$, alors, $\frac{1}{q} \leqslant \frac{1}{q_n}$. Par suite,

$$\frac{1}{q}+\frac{1}{q_n} \leqslant \frac{2}{q_n}.$$

En utilisant cette inégalité et l'inégalité (1.42), l'inégalité (1.41) devient comme suit :

$$\left|\frac{p}{q}-\frac{p_n}{q_n}\right| < \frac{1}{qq_n}.$$

Par conséquent,

$$\left|pq_n-qp_n\right| < 1.$$

Comme p, q, p_n et q_n sont des entiers, alors $|pq_n - qp_n| = 0$. D'où $\frac{p}{q} = \frac{p_n}{q_n}$. Ainsi la preuve est achevée. □

1.5 Développement en fraction continue d'un irrationnel quadratique

Nous étudions dans cette section le développement en fraction continue des nombres irrationnels qui sont racines d'un polynôme de degré 2, et à coefficients rationnels.

Définition 1.31. *Un nombre irrationnel x est dit quadratique s'il est racine d'un polynôme de degré 2, à coefficients rationnels.*

Exemple 1.32. *Soit d un entier strictement positif et non carré. L'irrationnel $\sqrt{d}$ est racine du polynôme $P(X) = X^2 - d$, qui est à coefficients entiers. Par conséquent, $\sqrt{d}$ est quadratique.*

Dans la suite, nous considérons un nombre irrationnel x et les suites $(a_n)_{n\geqslant 0}$, $(x_n)_{n\geqslant 0}$ définies par (1.25).

Définition 1.33. *Le développement en fraction continue de x est dit périodique, s'il existe deux entiers $k \geqslant 0$ et $m \geqslant 1$ tels que*

$$\forall n \geqslant k, \quad a_{n+m} = a_n. \tag{1.43}$$

Le plus petit entier m strictement positif vérifiant la relation (1.43) s'appelle la période du développement en fraction continue de x. Dans le cas particulier $k = 0$, le développement en fraction continue de x est dit purement périodique.

Notation 1.34. *Le développement en fraction continue de x se note comme suit :*

$$x = \left[a_0, \ldots, a_{k-1}, \overline{a_k, \ldots, a_{k+m-1}}\right], \tag{1.44}$$

où la barre placée au dessus des termes a_k,..., a_{k+m-1} signifie que ces derniers se répètent indéfiniment.

Le lemme suivant nous sera utile lors de la démonstration de la proposition 1.36.

Lemme 1.35. *Soient ℓ un entier naturel et $(y_n)_{n\geqslant 0}$ la suite définie par $y_0 = x_\ell$ et pour tout entier $n \geqslant 0$,*

$$y_{n+1} = \frac{1}{y_n - \lfloor y_n \rfloor}.$$

Alors pour tout entier $n \geqslant 0$, $y_n = x_{n+\ell}$.

Démonstration. Prouvons que pour tout entier $n \geqslant 0$, $y_n = x_{n+\ell}$.

— Nous avons $y_0 = x_\ell$. Donc la relation est vérifiée pour $n = 0$.

— Fixons $n \geqslant 0$. Supposons que $y_n = x_{n+\ell}$ et montrons que $y_{n+1} = x_{n+1+\ell}$. Comme pour tout entier $n \geqslant 0$,

$$y_{n+1} = \frac{1}{y_n - \lfloor y_n \rfloor},$$

alors en utilisant l'hypothèse de récurrence, nous obtenons

$$y_{n+1} = \frac{1}{x_{n+\ell} - \lfloor x_{n+\ell} \rfloor}.$$

La relation (1.25) nous permet de déduire que $y_{n+1} = x_{n+1+\ell}$.
Conclusion : Par le principe de récurrence, on a pour tout entier $n \geqslant 0$, $y_n = x_{n+\ell}$. □

Proposition 1.36. *Si le développement en fraction continue de x est périodique de période $m \geqslant 1$, à partir d'un certain rang $k \geqslant 0$, alors*

1. *le développement en fraction continue de x_k est purement périodique,*
2. $x_{m+k} = x_k$,
3. *la suite $(x_n)_{n\geqslant 0}$ est périodique de période m à partir du rang k.*

Démonstration.

1. Considérons les suites $(b_n)_{n\geqslant 0}$ et $(y_n)_{n\geqslant 0}$ définies par $y_0 = x_k$ et pour tout $n \geqslant 0$

$$b_n = \lfloor y_n \rfloor \text{ et } y_{n+1} = \frac{1}{y_n - \lfloor y_n \rfloor}. \tag{1.45}$$

D'après le lemme 1.35 pour tout entier $n \geqslant 0$,

$$y_n = x_{n+k}.$$

Donc, en utilisant les relations (1.45) et (1.25), nous obtenons que pour tout $n \geqslant 0$,

$$b_n = a_{n+k}.$$

Par suite, pour tout entier $n \geqslant 0$,

$$b_{n+m} = a_{n+m+k}. \tag{1.46}$$

Puisque $n + k \geqslant k$, et par hypothèse le développement en fraction continue de x est périodique de période $m \geqslant 1$, à partir du rang $k \geqslant 0$, alors d'après la définition 1.33,

$$a_{n+k+m} = a_{n+k}.$$

Par conséquent, pour tout entier $n \geqslant 0$,

$$b_{n+m} = b_n. \tag{1.47}$$

Ce qui signifie que le développement en fraction continue de x_k est purement périodique.

2. Considérons les suites $(c_n)_{n\geqslant 0}$ et $(z_n)_{n\geqslant 0}$ définies par $z_0 = x_{m+k}$ et pour tout $n \geqslant 0$

$$c_n = \lfloor z_n \rfloor \text{ et } z_{n+1} = \frac{1}{z_n - \lfloor z_n \rfloor}. \tag{1.48}$$

D'après le lemme 1.35, pour tout entier $n \geqslant 0$, $z_n = x_{n+m+k}$. Alors, en utilisant les relations (1.48) et (1.25), on obtient : $c_n = a_{n+m+k}$. Les relation (1.46) et (1.47) nous permettent de déduire que pour tout $n \geqslant 0$,

$$b_n = c_n.$$

Comme d'après la seconde assertion de la proposition 1.26,

$$x_k = \lim_{n\to+\infty} F_n(b_0, \ldots, b_n) \text{ et } x_{m+k} = \lim_{n\to+\infty} F_n(c_0, \ldots, c_n),$$

alors $x_{m+k} = x_k$.

3. Prouvons la dernière assertion. Commençons par montrer que

$$\forall n \geqslant k, \quad x_{n+m} = x_n. \tag{1.49}$$

— D'après la seconde assertion, $x_{m+k} = x_k$. Ainsi la relation est vérifiée pour $n = k$.
— Fixons $n \geqslant k$. Supposons que $x_{n+m} = x_n$, et montrons que $x_{n+1+m} = x_{n+1}$. Nous avons par la relation (1.25),

$$x_{n+m+1} = \frac{1}{x_{n+m} - \lfloor x_{n+m} \rfloor}.$$

En utilisant l'hypothèse de récurrence, nous obtenons

$$x_{n+m+1} = \frac{1}{x_n - \lfloor x_n \rfloor}.$$

En utilisant à nouveau la relation (1.25), nous obtenons :

$$x_{n+m+1} = x_{n+1}.$$

Conclusion : Par le principe de récurrence, on a pour tout $n \geqslant k$, $x_{n+m} = x_n$.
Pour finir, montrons que m est le plus petit entier strictement positif vérifiant la relation (1.49).
— **Cas 1** : $m = 1$. Il est clair que m est la période de la suite $(x_n)_{n\geqslant 0}$.
— **Cas 2** : $m \geqslant 2$. Supposons qu'il existe un entier $\ell \in \{1, \ldots, m-1\}$ tel que pour tout entier $n \geqslant k$, $x_{n+\ell} = x_n$. Donc, en utilisant la relation (1.25), on obtient que pour tout entier $n \geqslant k$, $a_{n+\ell} = a_n$. Ce qui contredit le fait que m est la période de la suite $(a_n)_{n\geqslant 0}$.

□

Il est clair que si le développement en fraction continue de x est purement périodique, de période $m \geqslant 1$, alors $x = x_m$. Ce qui entraîne que $x > 1$. Cette condition n'est pas suffisante. En effet, le lemme 1.39, montre que le conjugué de x est nécessairement compris entre -1 et 0.

Définition 1.37. *Si α est un irrationnel quadratique et β son conjugué, alors α est dit quadratique réduit si $\alpha > 1$ et $-1 < \beta < 0$.*

Exemple 1.38. *Soit d est un entier strictement positif et non carré. Posons $\alpha = \left\lfloor \sqrt{d} \right\rfloor + \sqrt{d}$. Alors $\alpha \in \mathbb{Q}\left(\sqrt{d}\right)$. Il en résulte que l'irrationnel α est quadratique. Comme $\sqrt{d} > 1$, alors $\left\lfloor \sqrt{d} \right\rfloor \geqslant 1$. Par suite, $\alpha > 1$.*
Soit $\beta = \left\lfloor \sqrt{d} \right\rfloor - \sqrt{d}$, le conjugué de α. Puisque $\sqrt{d} = \left\lfloor \sqrt{d} \right\rfloor + \left\{ \sqrt{d} \right\}$, alors $\beta = -\left\{ \sqrt{d} \right\}$. Par conséquent, $-1 < \beta < 0$. Nous remarquons que α et β vérifient les conditions de la définition ci-dessus. Ce qui signifie que α est un irrationnel quadratique réduit.

Lemme 1.39. *Si le développement en fraction continue de x est purement périodique alors x est réduit.*

Démonstration. Comme le développement en fraction continue de x est par hypothèse purement périodique, alors d'après la troisième assertion de la proposition 1.36, $x_m = x_0 = x$. Puisque $m \in \mathbb{N}^*$, alors deux cas se présentent :

- **Cas 1** : $m = 1$. En utilisant la relation (1.4), nous obtenons $x = \dfrac{a_0 x + 1}{x}$. Par suite, $x^2 - a_0 x - 1 = 0$. Par conséquent, x est racine du polynôme $f(X) = X^2 - a_0 X - 1 \in \mathbb{Z}[X]$. Vu que $x = x_1 > 1$, alors $a_0 = \lfloor x \rfloor \geqslant 1$. D'où $f(-1) = a_0 > 0$. Comme $f(0) = -1 < 0$, alors f admet une racine dans l'intervalle $]-1;\ 0[$. Ce qui signifie que x est réduit
- **Cas 2** : $m \geqslant 2$. En utilisant le lemme 1.25 et le fait que $x_m = x$, nous obtenons :

$$x = \frac{x p_{m-1} + p_{m-2}}{x q_{m-1} + q_{m-2}}.$$

Donc x est racine du polynôme $g(X) = q_{m-1} X^2 + (q_{m-2} - p_{m-1}) X - p_{m-2} \in \mathbb{Z}[X]$. On a d'un côté $x = x_m > 1$ donc, en utilisant les propositions 1.11 et 1.13, on trouve que $g(0) = -p_{m-2} < 0$ et $g(-1) = (p_{m-1} - p_{m-2}) + (q_{m-1} - q_{m-2}) > 0$. D'où g admet une racine dans l'intervalle $]-1;\ 0[$. Autrement dit, x est réduit.

□

Le théorème suivant a été démontré par Leonhard Euler.

Théorème 1.40 ([17])**.** *Si le développement en fraction continue de x est périodique alors x est un nombre irrationnel quadratique.*

Démonstration. Nous avons deux cas à traiter.

- **Cas 1** : Le développement en fraction continue de x est purement périodique. Dans ce cas, d'après le lemme 1.39, x est un nombre irrationnel quadratique réduit.
- **Cas 2** : Le développement en fraction continue de x est périodique de période $m \geqslant 1$, à partir d'un certain rang $k \geqslant 1$.
  - Si $k = 1$, alors d'après la troisième assertion de la proposition 1.23, $x = F_1(a_0, x_1)$. En utilisant la relation (1.3), nous obtenons $x = a_0 + \dfrac{1}{x_1}$. D'après la première assertion de la proposition 1.36, le développement en fraction continue de x_1 est purement

périodique. Donc, d'après le lemme 1.39, x est un nombre irrationnel quadratique. Comme $x = a_0 + \dfrac{1}{x_1}$, alors $x \in \mathbb{Q}(x_1)$. Par conséquent, x est quadratique.

— Si $k \geqslant 2$, alors en utilisant le lemme 1.25, nous obtenons

$$x = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}}.$$

Le développement en fraction continue de x_k est en vertu de la première assertion de la proposition 1.36 purement périodique. Donc, selon le lemme 1.39, x_k est un irrationnel quadratique. Puisque p_{k-1}, p_{k-2}, q_{k-1}, et q_{k-2} sont des entiers, alors $x \in \mathbb{Q}(x_k)$. Par conséquent, il est quadratique.

□

Le théorème suivant dû à Joseph-Louis Lagrange montre que la réciproque du théorème 1.40 est vraie.

Théorème 1.41 ([17])**.** *Si x est un irrationnel quadratique, alors son développement en fraction continue est périodique.*

Pour la preuve nous aurons besoin du lemme suivant.

Lemme 1.42. *S'il existe deux entiers naturels r et s tels que $r > s$ et $x_r = x_s$, alors le développement en fraction continue de x est périodique.*

Démonstration. Commençons par prouver que pour tout entier $n \geqslant s$, $x_{n+r-s} = x_n$.

— Comme par hypothèse $x_r = x_s$, alors la formule est vérifiée pour $n = s$.

— Fixons $n \geqslant s$. Supposons que $x_{n+r-s} = x_n$, et montrons que $x_{n+1+r-s} = x_{n+1}$. D'après la relation (1.25),

$$x_{n+1+r-s} = \frac{1}{x_{n+r-s} - \lfloor x_{n+r-s} \rfloor}.$$

En utilisant l'hypothèse de récurrence, ensuite la relation (1.25), nous obtenons

$$x_{n+1+r-s} = x_{n+1}.$$

Conclusion : Par le principe de récurrence, on a pour tout entier $n \geqslant s$, $x_{n+r-s} = x_n$.
En utilisant la relation (1.25), nous obtenons que pour tout entier $n \geqslant s$, $a_{n+r-s} = a_n$. Par conséquent, le développement en fraction continue de x est périodique. □

Démonstration du théorème 1.41. Comme x est supposé quadratique, alors il existe des entiers a, b et c tels que

$$ax^2 + bx + c = 0. \tag{1.50}$$

D'après la première assertion du lemme 1.25, pour tout entier $n \geqslant 1$,

$$x = \frac{x_{n+1} p_n + p_{n-1}}{x_{n+1} q_n + q_{n-1}}.$$

Par conséquent,

$$a\left(\frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}\right)^2 + b\left(\frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}\right) + c = 0.$$

En faisant les calculs nécessaires, nous trouvons que pour tout entier $n \geqslant 1$, x_{n+1} est racine du polynôme $A_{n+1}X^2 + B_{n+1}X + C_{n+1}$ où,

$$A_{n+1} = ap_n^2 + bp_nq_n + cq_n^2, \tag{1.51}$$
$$B_{n+1} = 2ap_np_{n-1} + b(p_nq_{n-1} + q_np_{n-1}) + 2cq_nq_{n-1}, \tag{1.52}$$
$$C_{n+1} = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2. \tag{1.53}$$

Selon la première assertion de la proposition 1.26, pour tout entier $n \geqslant 0$,

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

Comme d'après la proposition 1.13, la suite $(q_n)_{n\geqslant 0}$ est une suite d'entiers strictement positifs, alors, pour tout entier $n \geqslant 0$,

$$|xq_n - p_n| < \frac{1}{q_n}.$$

Posons $\epsilon = (p_n - xq_n)q_n$. Alors d'après ce qui précède, $|\epsilon| < 1$ et

$$\forall n \geqslant 0, \quad p_n = xq_n + \frac{\epsilon}{q_n}. \tag{1.54}$$

D'où,

$$A_{n+1} = (ax^2 + bx + c)q_n^2 + \epsilon(2ax + b) + a\left(\frac{\epsilon}{q_n}\right)^2.$$

En utilisant (1.50), nous obtenons

$$A_{n+1} = \epsilon(2ax + b) + a\left(\frac{\epsilon}{q_n}\right)^2.$$

Par suite,

$$|A_{n+1}| \leqslant |\epsilon||2ax + b| + |a|\left(\left|\frac{\epsilon}{q_n}\right|\right)^2.$$

Comme $|\epsilon| < 1$ et d'après le lemme 1.12, $q_n \geqslant n \geqslant 1$, alors

$$\forall n \geqslant 1, \quad |A_{n+1}| < |2ax + b| + |a|. \tag{1.55}$$

Nous remarquons à partir des relations (1.51) et (1.53) que $C_{n+2} = A_{n+1}$. Donc

$$\forall n \geqslant 1, \quad |C_{n+2}| < |2ax + b| + |a|. \tag{1.56}$$

Comme $q_0 = 1$ et par la relation (1.54) $p_0 = xq_0 + \frac{\epsilon}{q_0}$, alors en utilisant la relation (1.53)

on obtient que $C_2 = (2ax + b)\epsilon + a\epsilon^2$. En prenant en considération le fait que $|\epsilon| < 1$, nous obtenons l'inégalité suivante : $|C_2| < |2ax + b| + |a|$. Il résulte de cela et de la relation (1.56) que

$$\forall n \geqslant 1, \quad |C_{n+1}| < |2ax + b| + |a|. \tag{1.57}$$

En utilisant les relations (1.51),(1.52) et (1.53) nous obtenons

$$B_{n+1}^2 - 4A_{n+1}C_{n+1} = (b^2 - 4ac)(p_n q_{n-1} - p_{n-1}q_n)^2.$$

La relation donnée par la première assertion du lemme 1.9 nous permet de déduire que pour tout entier $n \geqslant 1$,

$$B_{n+1}^2 - 4A_{n+1}C_{n+1} = b^2 - 4ac.$$

Par conséquent, comme les relations (1.55) et (1.57) montrent que les suites $(A_{n+1})_{n\geqslant 1}$ et $(C_{n+1})_{n\geqslant 1}$ sont bornées, alors il en est de même pour la suite $(B_{n+1})_{n\geqslant 1}$. Étant donné que pour tout entier $n \geqslant 1$, A_{n+1},B_{n+1},C_{n+1} sont des entiers, alors l'ensemble

$$\{A_{n+1}, B_{n+1}, C_{n+1} \mid n \in \mathbb{N}^*\}$$

est fini. Il en résulte que l'ensemble des polynômes, $A_{n+1}X^2 + B_{n+1}X + C_{n+1}$, où $n \in \mathbb{N}^*$ est fini. Par conséquent, $\{x_{n+1} \mid n \in \mathbb{N}^*\}$ est également fini. D'où l'existence de deux entiers r et s tels que $r > s$ et $x_r = x_s$. D'après le lemme 1.42, le développement en fraction continue de x est périodique. □

Les théorèmes 1.40 et 1.41 dûs respectivement à Leonhard Euler et Joseph Louis de Lagrange, nous permettent de conclure qu'un nombre irrationnel est quadratique si et seulement si son développement en fraction continue est périodique. La question qui s'impose naturellement est celle de savoir à quelle condition le développement est purement périodique ? La réponse à cette question a été donnée par Evariste Galois [6] en 1828.

Théorème 1.43 ([17])**.** *Si l'irrationnel x est quadratique réduit, alors son développement en fraction continue est purement périodique.*

La démonstration de ce théorème nécessite quelques résultats que nous présenterons sous forme de lemmes.

Lemme 1.44. *Si l'irrationnel x est quadratique, alors*

1. *pour tout entier $n \geqslant 0$, x_n est un irrationnel quadratique.*
2. *Si pour tout $n \geqslant 0$, y_n est le conjugué de x_n, alors*

$$y_n = a_n + \frac{1}{y_{n+1}}.$$

Démonstration.

1. D'après la relation (1.25), pour tout $n \geqslant 0$,

$$x_n = \lfloor x_n \rfloor + \frac{1}{x_{n+1}} \quad \text{et} \quad x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor}.$$

   Donc, pour tout $n \geqslant 0$, $\mathbb{Q}(x_n) = \mathbb{Q}(x_{n+1})$. Autrement dit pour tout $n \geqslant 0$, $\mathbb{Q}(x_n) = \mathbb{Q}(x_0)$. Comme $x_0 = x$ et x est par hypothèse quadratique, alors x_n l'est également.

2. Soit y le conjugué de x et σ l'unique $\mathbb{Q}$-automorphisme de corps de $\mathbb{Q}(x)$ vérifiant pour tous $a, b \in \mathbb{Q}$, $\sigma(a + bx) = a + by$. Par suite, pour tout entier $n \geqslant 0$, $y_n = \sigma(x_n)$. Donc en utilisant la relation (1.25), nous obtenons

$$y_n = \sigma\left(a_n + \frac{1}{x_{n+1}}\right).$$

   Par conséquent, pour tout entier $n \geqslant 0$,

$$\begin{aligned} y_n &= a_n + \frac{1}{\sigma(x_{n+1})} \\ &= a_n + \frac{1}{y_{n+1}}. \end{aligned}$$

Ce qui termine la preuve. □

Lemme 1.45. *Si l'irrationnel x est quadratique réduit, alors pour tout entier $n \geqslant 0$, x_n est un nombre irrationnel quadratique réduit.*

Démonstration. Comme $x = x_0$, et est par hypothèse quadratique réduit, alors $x_0 > 1$. Donc d'après la proposition 1.23, pour tout entier $n \geqslant 0$, x_n est un nombre irrationnel supérieur à 1. Et d'après la première assertion du lemme 1.44, pour tout entier $n \geqslant 0$, x_n est quadratique. Donc pour montrer que x_n est quadratique réduit, il suffit de montrer que son conjugué, noté y_n est dans l'intervalle $]-1; 0[$ pour tout entier $n \geqslant 0$. Pour ce faire, nous allons procéder par récurrence.

— Comme $x = x_0$, et est par hypothèse quadratique réduit, alors $-1 < y_0 < 0$.

— Fixons $n \geqslant 0$. Supposons que $-1 < y_n < 0$ et montrons que $-1 < y_{n+1} < 0$. En utilisant à nouveau la relation donnée par la seconde assertion du lemme 1.44, nous obtenons

$$y_{n+1} = \frac{1}{y_n - a_n}.$$

  En utilisant l'hypothèse de récurrence, nous obtenons les inégalités suivantes :

$$-1 - a_n < y_n - a_n < -a_n.$$

  On $a_0 = \lfloor x \rfloor = 0$. Comme $x_0 > 1$, alors $a_0 \geqslant 1$ et d'après la seconde assertion de la proposition 1.23, $a_n \geqslant 1$, pour tout entier $n \geqslant 1$. Autrement dit, pour tout $n \geqslant 0$,

$a_n \geqslant 1$. Cela nous permet de déduire que pour tout entier $n \geqslant 1$,

$$y_n - a_n < -1.$$

Par conséquent,

$$-1 < y_{n+1} < 0.$$

Conclusion : Par le principe de récurrence, on a pour tout entier $n \geqslant 1$, $-1 < y_n < 0$. □

Nous pouvons à présent donner la preuve du théorème 1.43.

Démonstration du théorème 1.43. Supposons que x est un irrationnel quadratique réduit. Donc, d'après le théorème 1.41, le développement en fraction continue de x est périodique à partir d'un certain rang. Soient m la période de la suite $(a_n)_{n\geqslant 0}$ et k le plus petit entier positif vérifiant :

$$\forall n \geqslant k, a_{n+m} = a_n.$$

Montrons que $k = 0$. Pour cela nous allons procéder par l'absurde en supposant $k \geqslant 1$. Vu que x est quadratique, alors d'après la seconde assertion du lemme 1.44,

$$y_{k-1} - y_{k-1+m} = a_{k-1} + \frac{1}{y_k} - a_{k-1+m} - \frac{1}{y_{k+m}}. \tag{1.58}$$

Puisque le développement en fraction continue de x est supposé périodique de période $m \geqslant 1$, alors d'après la seconde assertion de la proposition 1.36, $x_{m+k} = x_k$. Par conséquent, y_k le conjugué de x_k et y_{m+k} le conjugué de x_k sont égaux. Donc, l'égalité (1.58) devient comme suit

$$y_{k-1} - y_{k-1+m} = a_{k-1} - a_{k-1+m}. \tag{1.59}$$

Comme x est par hypothèse un nombre irrationnel quadratique réduit, alors par le lemme 1.45, $-1 < y_{k-1} < 0$, et $-1 < y_{k-1+m} < 0$. Donc $-1 < y_{k-1} - y_{k-1+m} < 1$. La relation (1.59) nous permet de déduire que $-1 < a_{k-1+m} - a_{k-1} < 1$. Puisque a_{k-1} et a_{k-1+m} sont des entiers, alors

$$a_{k-1+m} - a_{k-1} = 0.$$

Ce qui contredit la minimalité de k, c'est-à-dire $k = 0$. Par conséquent, le développement en fraction continue de x est purement périodique. □

Proposition 1.46. *Le développement en fraction continue de $\sqrt{d}$ est périodique à partir du premier rang. Autrement dit, il existe un entier $m \geqslant 1$ tel que*

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

Démonstration. Posons $y_0 = \sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor$. Considérons les suites $(b_n)_{n\geqslant 0}$ et $(y_n)_{n\geqslant 0}$ définies pour tout $n \geqslant 0$ par $b_n = \lfloor y_n \rfloor$ et $y_{n+1} = \frac{1}{y_n - \lfloor y_n \rfloor}$. D'après la proposition 1.26,

$$\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor = \lim_{n\to+\infty} F_n(b_0, \ldots, b_n).$$

Par suite,

$$\sqrt{d} = -\left\lfloor \sqrt{d} \right\rfloor + \lim_{n\to+\infty} F_n(b_0, \ldots, b_n).$$

En utilisant la proposition 1.1, nous obtenons

$$\sqrt{d} = -\left\lfloor \sqrt{d} \right\rfloor + \lim_{n\to+\infty} \left(b_0 + \frac{1}{F_{n-1}(b_1, \ldots, b_n)} \right).$$

Donc,

$$\sqrt{d} = \lim_{n\to+\infty} \left(-\left\lfloor \sqrt{d} \right\rfloor + b_0 + \frac{1}{F_{n-1}(b_1, \ldots, b_n)} \right).$$

En utilisant à nouveau la proposition 1.1, nous obtenons ce qui suit :

$$\sqrt{d} = \lim_{n\to+\infty} F_n \left(b_0 - \left\lfloor \sqrt{d} \right\rfloor, b_1, \ldots, b_n \right).$$

Posons $a_0 = b_0 - \left\lfloor \sqrt{d} \right\rfloor$ et pour tout entier $n \geqslant 1$, $a_n = b_n$. Alors

$$\sqrt{d} = \lim_{n\to+\infty} F_n \left(a_0, a_1, \ldots, a_n \right).$$

Nous avons obtenu ainsi le développement en fraction continue de $\sqrt{d}$.
D'après l'exemple 1.38, $\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor$ est un nombre irrationnel réduit. Donc, d'après le théorème 1.43, son développement en fraction continue est purement périodique. Soit m sa période. Alors pour tout entier $n \geqslant 0$, $b_{n+m} = b_n$. D'une part, vu que pour tout entier $n \geqslant 1$, $a_n = b_n$, alors le développement en fraction continue de $\sqrt{d}$ est périodique de période m à partir de $k = 1$. D'autre part, $a_m = b_m = b_0$ et comme $b_0 = \left\lfloor \sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor \right\rfloor = 2 \left\lfloor \sqrt{d} \right\rfloor$, alors

$$a_0 = b_0 - \left\lfloor \sqrt{d} \right\rfloor = \frac{1}{2} b_0.$$

Par conséquent $a_m = b_m = b_0 = 2a_0$. En utilisant la notation (1.44), nous obtenons :

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

Ce qui achève la preuve. □

Nous clôturons ce chapitre par donner le développement en fraction continue de $\sqrt{17}$ et celui de $\sqrt{6083}$ ainsi que quelques unes de leurs réduites.

Exemple 1.47.

— *Posons* $x_0 = \sqrt{17}$*, alors d'après la relation* (1.25)*,* $a_0 = \left\lfloor \sqrt{17} \right\rfloor = 4$*. Poursuivons le calcul en utilisant la relation* (1.25)*. Nous avons*

$$x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{17} - 4} = \sqrt{17} + 4, \ \textit{donc,}\ a_1 = 8.$$
$$x_2 = \frac{1}{x_1 - a_1} = \frac{1}{\sqrt{17} - 4} = x_1, \ \textit{donc,}\ a_2 = a_1 = 8.$$

Comme $x_2 = x_1$ alors pour tout $n \geqslant 1$, $x_{n+1} = x_n$. Autrement dit le développement en fraction continue de $\sqrt{17}$ est périodique de période $m = 1$ à partir du rang $k = 1$. Donc en utilisant la notation (1.44)*, nous obtenons $\sqrt{17} = \left[4, \overline{8}\right]$.*

— *Passons au calcul de quelques réduites. Comme $a_0 = 4$ et $a_1 = 8$, alors en utilisant les relations* (1.27) *et* (1.29)*, nous obtenons ce qui suit :*

$$p_0 = 4,\ p_1 = 33,\ q_0 = 1,\ et\, q_1 = 8,.$$

Par conséquent,

$$\frac{p_0}{q_0} = 4, \quad et \quad \frac{p_1}{q_1} = \frac{33}{8}.$$

Exemple 1.48.

— *Posons $x_0 = \sqrt{6083}$. D'après la relation* (1.25)*, $a_0 = \left\lfloor \sqrt{6083} \right\rfloor = 77$. Poursuivons le calcul en utilisant la relation* (1.25)*. On a*

$$x_1 = \frac{1}{x_0 - a_0} = \frac{1}{\sqrt{6083} - 77} = \frac{77 + \sqrt{6083}}{154}.$$

Puisque $77 < \sqrt{6083} < 78$, donc

$$1 = \frac{77 + 77}{154} < x_1 < \frac{77 + 78}{154} = \frac{155}{154}.$$

Par conséquent $a_1 = 1$.

$$x_2 = \frac{1}{x_1 - a_1} = 77 + \sqrt{6083},\ \ donc,\ a_2 = 154.$$
$$x_3 = \frac{1}{x_2 - a_2} = \frac{1}{\sqrt{6083} - 77} = x_1,\ \ donc,\ a_3 = a_1 = 1.$$

Comme $x_3 = x_1$ alors pour tout $n \geqslant 1$, $x_{n+2} = x_n$. Autrement dit le développement en fraction continue de $\sqrt{6083}$ est périodique de période $m = 2$ à partir du rang $k = 1$. Donc en utilisant la notation (1.44)*, nous obtenons $\sqrt{6083} = \left[77, \overline{1, 154}\right]$.*

— *Calculons quelques réduites. Comme $a_0 = 77$ et $a_1 = 1$, alors en utilisant les relations* (1.27) *et* (1.29)*, nous obtenons ce qui suit :*

$$\frac{p_0}{q_0} = 77 \quad et \quad \frac{p_1}{q_1} = \frac{78}{1}.$$

Chapitre 2

L'équation de Pell-Fermat

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

$$u^2 - dv^2 = 1, \tag{2.1}$$

où d est un entier strictement positif et non carré. Il est clair que les couples $(-1, 0)$ et $(1, 0)$ sont des solutions de l'équation de Pell-Fermat (2.1). Ces dernières sont appelées solutions triviales. Il faut noter que généralement, cette équation est appelée équation de Pell. Cette dénomination est due à Euler, alors que historiquement, le mathématicien anglais John Pell (1611–1685) n'a apparemment pas contribué à sa résolution.
Plusieurs mathématiciens se sont intéressés à l'étude de cette équation, tel que le mathématicien indien Brahmagupta (598-670). Nous pouvons également citer les mathématiciens anglais John Wallis (1616–1703) et William Brouncker (1620–1684), qui ont été défiés en 1657 par Pierre de Fermat à prouver que l'équation (2.1) admet une infinité de solutions entières non triviales.
En 1730, Leonhard Euler (1707-1783) a repris l'étude de cette équation et il a démontré comment obtenir un ensemble infini de solutions à partir d'une solution non triviale, supposée connue. Et il a aussi trouver son lien avec les fractions continues. Mais, il n'a pas démontré l'existence d'au moins une solution entière non triviale. C'est Joseph-Louis Lagrange (1736-1813) qui a résolu ce problème en prouvant que l'équation de Pell-Fermat admet toujours des solutions entières. Pour cela, il a utilisé le développement en fraction continue de l'irrationnel $\sqrt{d}$. Il a prouvé que les solutions à coordonnées positives de l'équation de Pell-Fermat se trouvent parmi les couples (p_n, q_n), où $\frac{p_n}{q_n}$ est une réduite de $\sqrt{d}$ et n un entier positif.

Le présent chapitre est composé de quatre parties. Dans la première partie, en suivant le procédé de Lagrange basé sur le développement en fraction continue de $\sqrt{d}$, nous prouverons que l'équation de Pell-Fermat admet une infinité de solutions à coordonnées positives. Nous prouverons également que parmi ces dernières, il existe une solution (x_1, y_1), souvent appelée solution minimale ou fondamentale, vérifiant la propriété suivante : Étant donné un couple solution (x, y) à coordonnées positives de l'équation de Pell-Fermat (2.1), alors $x \geqslant x_1$ et

$y \geqslant y_1$. Ensuite, en posant pour tout entier $k \geqslant 0$,

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k,$$

nous prouverons que l'ensemble des solutions à coordonnées positives de l'équation de Pell-Fermat est composé des couples (x_k, y_k). Il en résulte de cela que toutes les solutions à coordonnées positives s'obtiennent à partir de la solution minimale (x_1, y_1).
Dans la seconde partie, en utilisant la relation ci-dessus, nous démontrerons plusieurs relations vérifiées par les solutions à coordonnées positives de l'équation de Pell-Fermat (2.1). Parmi celles-ci, les deux suivantes : pour tout entier $k \geqslant 0$,

$$x_{k+2} = 2x_1x_{k+1} - x_k \text{ et } x_{2k} = 2x_k^2 - 1.$$

Enfin, nous donnerons deux lemmes concernant les solutions (x_k, y_k), dont l'intérêt se verra dans le chapitre à venir. Dans la troisième partie, nous verrons qu'il y a un lien entre les solutions à coordonnées positives de l'équation de Pell-Fermant et les polynômes de Tchebychev de première et seconde espèce. Dans la quatrième partie, nous [1] donnerons de nouveaux résultats concernant la suite $(x_k)_{k\geqslant 0}$. Ces derniers seront utilisés dans les démonstrations des différents théorèmes du dernier chapitre.

Pour la partie histoire de cette introduction nous nous sommes inspirés du livre [9] et de l'article de Bureaux-Bourgois [4]. En ce qui concerne le reste du chapitre, nous nous sommes inspirés des livres suivants : [2], [9] et[20].

2.1 Résolution de l'équation de Pell-Fermat

Notre but est de montrer que l'équation de Pell-Fermat admet une infinité de solutions non triviales. Mais avant cela, traitons quelques cas particulier afin de justifier l'hypothèse d positif et non carré. Soit (x, y) une solution à coordonnées entières de l'équation

$$u^2 - dv^2 = 1.$$

— Si $d = 0$, alors $x^2 = 1$. Par conséquent, l'équation $u^2 - dv^2 = 1$ admet une infinité de solutions, celles-ci sont de la forme $(\pm 1, y)$, avec $y \in \mathbb{Z}$.
— Si $d = -1$ alors $(\pm 1, 0), (0, \pm 1)$ sont les seules solutions de l'équation $u^2 + v^2 = 1$.
— Si $d < -1$, alors $(\pm 1, 0)$ sont les seules solutions de l'équation $u^2 - dv^2 = 1$.
— Si $d = a^2$ avec $a \neq 0$, alors $x^2 - a^2y^2 = 1$ donne

$$(x - ay)(x + ay) = 1.$$

Comme x, y et a sont des entiers, alors deux cas se présentent :

$$\begin{cases} x - ay = 1 \\ x + ay = 1 \end{cases} \quad \text{ou} \quad \begin{cases} x - ay = -1 \\ x + ay = -1 \end{cases}.$$

Par conséquent $(x, y) = (1, 0)$ ou $(x, y) = (-1, 0)$.
Nous remarquons que pour ces valeurs de d, les solutions sont toutes connues, et c'est pour cette raison que nous les excluons. En d'autres termes, dans tout ce qui suit, on supposera que d est strictement positif et non carré.

Remarque 2.1. *Si (x, y) est solution de l'équation de Pell-Fermat, alors les couples $(x, -y)$, $(-x, y)$ et $(-x, -y)$ le sont également. Donc trouver les solutions à coordonnées positives suffit pour trouver toutes les solutions. C'est pourquoi nous allons chercher seulement les solutions (x, y), avec x et y positifs. Puisque x et y sont supposés positifs, alors c'est la solution $(1, 0)$ qui sera appelée dans toute la suite, solution triviale.*

Revenons à notre objectif initial, qui est de prouver que l'équation de Pell-Fermat (2.1) admet des solutions (x, y) non triviales. Nous commençons par donner un lemme dont l'intérêt se verra lors de la démonstration du théorème 2.3 ainsi que dans celle du théorème 2.4.

Lemme 2.2. *Soient x, y deux entiers naturels. Si (x, y) est un couple solution de l'équation de Pell-Fermat* (2.1)*, alors*

1. *x est strictement positif,*
2. *$x - y\sqrt{d} > 0$ et $x > y$,*
3. *x et y sont premiers entre eux.*

Démonstration.

1. Comme (x, y) est solution de l'équation de Pell-Fermat (2.1), alors $x^2 = 1 + dy^2$. Puisque $d > 1$, nous avons $x^2 \geqslant 1$. Comme x est supposé positif, alors $x \geqslant 1$.
2. Comme par hypothèse, $x^2 - dy^2 = 1$, alors

$$\left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right) = 1.$$

   Puisque $y \in \mathbb{N}$, $d > 1$ et d'après l'assertion (1), $x > 0$, alors $x + y\sqrt{d} > 0$. Ceci nous permet de déduire que $x - y\sqrt{d} > 0$. Pour finir, montrons que $x > y$. Puisque $x - y\sqrt{d} > 0$, alors $x > y\sqrt{d}$. Comme $y \in \mathbb{N}$ et $\sqrt{d} > 1$, alors $y\sqrt{d} \geqslant y$. D'où $x > y$.
3. Soit d' un diviseur commun à x et y, donc d' divise $x^2 - dy^2 = 1$. Par conséquent, x et y sont premiers entre eux.

□

D'après la proposition 1.46, $\sqrt{d}$ admet un développement en fraction continue périodique. Dans toute la suite m désigne la période du développement en fraction continue de $\sqrt{d}$, et pour tout entier $n \geqslant 0$, $\frac{p_n}{q_n}$ désigne la réduite d'ordre n de $\sqrt{d}$.
Dans l'introduction du présent chapitre, nous avons mentionné que les solutions de l'équation de Pell-Fermat se trouvent parmi les réduites de $\sqrt{d}$. Le théorème suivant nous éclaircit ce point.

Théorème 2.3 ([2])**.** *Soient x et y deux entiers strictement positifs. Si le couple (x, y) est solution de l'équation de Pell-Fermat* (2.1)*, alors il existe un entier $n \geqslant 0$ tels que, $x = p_n$ et $y = q_n$.*

Démonstration. Soit (x, y) une solution de l'équation de Pell-Fermat (2.1), avec x et y strictement positifs. Comme $\sqrt{d} > 1$ et $y > 0$, alors

$$y\sqrt{d} > y.$$

Puisque d'après la première assertion du lemme 2.2

$$x > y,$$

alors, $x + y\sqrt{d} > 2y$. D'où l'inégalité suivante :

$$\frac{1}{x + y\sqrt{d}} < \frac{1}{2y}. \tag{2.2}$$

Gardons cette inégalité de côté et revenons au fait que (x, y) soit un couple solution de l'équation de Pell-Fermat (2.1). Cela signifie que $\left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right) = 1$. D'où,

$$x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}}.$$

Par conséquent, en utilisant l'inégalité (2.2), nous obtenons :

$$x - y\sqrt{d} < \frac{1}{2y}.$$

Comme, d'après le lemme 2.2, $x - y\sqrt{d} > 0$, alors

$$\left|x - y\sqrt{d}\right| < \frac{1}{2y}.$$

Puisque y est par hypothèse strictement positif, alors

$$\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}.$$

Le théorème 1.28 nous affirme que la fraction $\frac{x}{y}$ est une réduite de $\sqrt{d}$. Autrement dit, il

existe un entier $n \geqslant 0$ tel que $\frac{x}{y} = \frac{p_n}{q_n}$. Rappelons que p_n et q_n sont d'après le corollaire 1.10 premiers entre eux, et x et y le sont également en vertu du lemme 2.2. Par conséquent $x = p_n$ et $y = q_n$. Ce qui termine la preuve. □

Il est naturel de se demander si pour tout entier $n \geqslant 0$, le couple (p_n, q_n), où $\frac{p_n}{q_n}$ est une réduite de $\sqrt{d}$, est solution de l'équation de Pell-Fermat (2.1) ? La réponse à été donnée par Joseph-Louis de Lagrange en 1768. Nous la présentons sous forme d'un théorème.

Théorème 2.4 ([2])**.** *Soit n un entier naturel. Le couple (p_n, q_n) est solution de l'équation de Pell-Fermat* (2.1) *si et seulement si n est impair et $m \mid n+1$.*

Pour la preuve nous nous sommes inspirés du livre d'Alan Baker [2].

Démonstration. Soit $n \in \mathbb{N}$. Selon la proposition 1.13, $q_n \in \mathbb{N}^*$. Puisque $a_0 = \lfloor \sqrt{d} \rfloor$ et $d > 1$, alors d'après la proposition 1.11, $p_n \in \mathbb{N}^*$. Par conséquent, en supposant que (p_n, q_n) est une solution de l'équation de Pell-Fermat (2.1), le lemme 2.2 nous fournit l'inégalité suivante : $p_n - q_n\sqrt{d} > 0$. Ce qui implique, $p_n > q_n\sqrt{d}$. En divisant cette inégalité par q_n, nous obtenons $\frac{p_n}{q_n} > \sqrt{d}$. Alors, en vertu de la troisième assertion de la proposition 1.26, n est impair. Prouvons que $m \mid (n+1)$. Comme $n \geqslant 1$, alors, d'après le lemme 1.25

$$\sqrt{d} = \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}.$$

Par suite,

$$\sqrt{d}\,(x_{n+1}q_n + q_{n-1}) = x_{n+1}p_n + p_{n-1}.$$

Et donc,

$$x_{n+1}\left(p_n - q_n\sqrt{d}\right) = q_{n-1}\sqrt{d} - p_{n-1}.$$

En multipliant par $p_n + q_n\sqrt{d}$, et en tenant compte du fait que (p_n, q_n) est par hypothèse une solution de l'équation de Pell-Fermat (2.1), nous obtenons :

$$x_{n+1} = \sqrt{d}\,(p_nq_{n-1} - q_np_{n-1}) + dq_nq_{n-1} - p_np_{n-1}.$$

En utilisant la première assertion du lemme 1.9, nous obtenons ce qui suit :

$$x_{n+1} = \sqrt{d}(-1)^{n+1} + dq_nq_{n-1} - p_np_{n-1}.$$

Puisque nous avons prouvé que l'entier n est impair, alors

$$x_{n+1} = \sqrt{d} + dq_nq_{n-1} - p_np_{n-1}.$$

Comme par la relation (1.25), $x_{n+1} = a_{n+1} + \frac{1}{x_{n+2}}$, et par la dernière assertion de la proposition 1.23, $\sqrt{d} = F_1(a_0, x_1) = a_0 + \frac{1}{x_1}$, alors

$$a_{n+1} + \frac{1}{x_{n+2}} = a_0 + \frac{1}{x_1} + dq_nq_{n-1} - p_np_{n-1}.$$

Par conséquent,

$$\frac{1}{x_{n+2}} - \frac{1}{x_1} = a_0 - a_{n+1} + dq_nq_{n-1} - p_np_{n-1}. \tag{2.3}$$

En utilisant la première assertion de la proposition 1.23, nous obtenons $-1 < \frac{1}{x_{n+2}} - \frac{1}{x_1} < 1$. Comme a_0 et a_{n+1} sont d'après la même proposition des entiers, et comme mentionné au début de cette preuve, p_n, p_{n-1}, q_n, et q_{n-1} sont également des entiers, alors en utilisant la relation (2.3) nous obtenons $\frac{1}{x_{n+2}} - \frac{1}{x_1} = 0$. Par conséquent, $x_{n+2} = x_1$.
Selon la proposition 1.46, le développement en fraction continue de $\sqrt{d}$ est périodique de période m à partir de $k = 1$. Par conséquent, d'après la troisième assertion du lemme 1.36, la suite $(x_n)_{n\geqslant 0}$ est périodique de période m à partir du rang $k = 1$. Ainsi, puisque $x_{n+2} = x_1$, alors il existe un entier $\ell \geqslant 1$ tel que $n + 2 = \ell m + 1$. Par conséquent, $m \mid n + 1$.
Réciproquement, supposons que n est impair et qu'il existe un entier $\ell \geqslant 1$ tel que $n+1 = \ell m$. Nous déduisons de la seconde hypothèse que $n+2 = \ell m+1$, et donc $x_{n+2} = x_{\ell m+1}$. Rappelons que la suite $(x_n)_{n\geqslant 0}$ est périodique de période m à partir de $k = 1$. Par conséquent $x_{n+2} = x_1$. D'après le lemme 1.25, $\sqrt{d}$ peut s'écrire comme suit :

$$\sqrt{d} = \frac{x_{n+2}p_{n+1} + p_n}{x_{n+2}q_{n+1} + q_n}.$$

Comme $x_{n+2} = x_1$, et d'après la relation (1.25), $x_1 = \frac{1}{\sqrt{d}-a_0}$, alors

$$\sqrt{d} = \frac{\left(\frac{1}{\sqrt{d}-a_0}\right) p_{n+1} + p_n}{\left(\frac{1}{\sqrt{d}-a_0}\right) q_{n+1} + q_n}.$$

En réduisant au même dénominateur, nous obtenons :

$$\sqrt{d} = \frac{p_{n+1} + p_n\left(\sqrt{d} - a_0\right)}{q_{n+1} + q_n\left(\sqrt{d} - a_0\right)}.$$

D'où,

$$\left(q_{n+1} + q_n\left(\sqrt{d} - a_0\right)\right)\sqrt{d} = p_{n+1} + p_n\left(\sqrt{d} - a_0\right).$$

En faisant les calculs nécessaires, nous obtenons :

$$\left(p_n + a_0q_n - q_{n+1}\right)\sqrt{d} = dq_n + a_0p_n - p_{n+1}.$$

Comme $\sqrt{d} \notin \mathbb{Q}$, alors $p_n + a_0q_n - q_{n+1} = dq_n + a_0p_n - p_{n+1} = 0$. Par conséquent,

$$p_n = -a_0q_n + q_{n+1} \text{ et } dq_n = -a_0p_n + p_{n+1}.$$

Par suite,

$$p_n^2 = (-a_0q_n + q_{n+1})p_n \text{ et } dq_n^2 = (-a_0p_n + p_{n+1})q_n.$$

Par conséquent,

$$p_n^2 - dq_n^2 = -\left(p_{n+1}q_n - q_{n+1}p_n\right)$$

En utilisant le lemme 1.9, et le fait que n est par hypothèse impair, nous obtenons,

$$p_n^2 - dq_n^2 = 1.$$

Donc le couple de coordonnées p_n et q_n est bien une solution de l'équation de Pell-Fermat (2.1).
□

Ce théorème nous permet de conclure que l'équation de Pell-Fermat possède une infinité de solutions non triviales à coordonnées positives. La proposition suivante, qui découle de ce théorème et du théorème 2.3 nous présente l'ensemble de ces solutions.

Proposition 2.5 ([9])**.**

- *Si m est pair, alors $S_1 = \{(p_{mk-1}, q_{mk-1}), k \in \mathbb{N}^*\}$ est l'ensemble des solutions à coordonnées strictement positives de l'équation de Pell-Fermat* (2.1).
- *Si m est impair, alors $S_2 = \{(p_{2mk-1}, q_{2mk-1}), k \in \mathbb{N}^*\}$ est l'ensemble des solutions à coordonnées strictement positives de l'équation de Pell-Fermat* (2.1).

Démonstration. D'après le théorème 2.3, toute solution à coordonnées strictement positives de l'équation de Pell-Fermat (2.1) est de la forme (p_n, q_n), où $\frac{p_n}{q_n}$ est une réduite de $\sqrt{d}$. Le théorème 2.4, quant à lui, montre que les couples (p_n, q_n) qui forment un couple solution de l'équation de Pell-Fermat sont ceux dont l'ordre n vérifie les conditions suivantes :

- n impair.
- $n+1$ divisible par m.

Par conséquent, ces solutions sont de la forme (p_{km-1}, q_{km-1}), avec $k \geqslant 1$. Mais comme d'après la première condition, $km-1$ doit être impair, alors deux cas se présentent :

- **Cas 1** : Si m est pair, alors $km-1$ est impair. Par conséquent, toute solution de l'équation de Pell-Fermat est de la forme (p_{km-1}, q_{km-1}), avec $k \geqslant 1$.
- **Cas 2** : Si m est impair alors $km-1$ est impair si et seulement si k est pair. D'où l'existence d'un entier strictement positif k', tel que, $k = 2k'$. Donc, les solutions de l'équation de Pell-Fermat sont de la forme $(p_{2k'm-1}, q_{2k'm-1})$.

□

Corollaire 2.6 ([9])**.** *Soit (x, y) une solution non-triviale à coordonnées positives de l'équation de Pell-Fermat* (2.1)*, on a :*

- *si m est pair, alors $x \geqslant p_{m-1}$ et $y \geqslant q_{m-1}$.*
- *Si m est impair, alors $x \geqslant p_{2m-1}$ et $y \geqslant q_{2m-1}$.*

Démonstration.

- **Cas 1** : Si m est pair, alors il existe d'après la proposition 2.5 un entier $k \geqslant 1$ tels que $x = p_{mk-1}$ et $y = q_{mk-1}$. Comme $k, m \geqslant 1$ alors

$$km - 1 \geqslant m - 1. \tag{2.4}$$

Vu que $\sqrt{d} > 1$, alors $a_0 = \lfloor \sqrt{d} \rfloor \geqslant 1$. Par conséquent, d'après les propositions 1.11 et 1.13, les suites $(p_n)_{n\geqslant 0}$ et $(q_n)_{n\geqslant 0}$ sont toutes les deux croissantes. Ainsi, la relation(2.4) nous permet de déduire que

$$p_{km-1} \geqslant p_{m-1} \quad \text{et} \quad q_{km-1} \geqslant q_{m-1}.$$

— **Cas 2** : Si m est impair, alors selon la proposition 2.5, il existe un entier $k \geqslant 1$, tels que $x = p_{2mk-1}$ et $y = q_{2mk-1}$. Étant donné que $k \geqslant 1$ et $m \geqslant 1$, alors $2mk - 1 \geqslant 2m - 1$. En utilisant à nouveau la croissance des suites $(p_n)_{n\geqslant 0}$ et $(q_n)_{n\geqslant 0}$, nous obtenons

$$p_{2km-1} \geqslant p_{2m-1} \quad \text{et} \quad q_{2km-1} \geqslant q_{2m-1}.$$

Ce qui termine la preuve. □

Définition 2.7. *La solution $(p_{\ell m-1}, q_{\ell m-1})$, où $\ell = 1$ si m est pair et $\ell = 2$ si m est impair, est appelée solution minimale de l'équation de Pell-Fermat* (2.1).

Posons maintenant pour tout entier $k \geqslant 0$,

$$x_k + y_k\sqrt{d} = (p_{\ell m-1} + q_{\ell m-1}\sqrt{d})^k. \tag{2.5}$$

Donc, (x_0, y_0) désigne la solution triviale de l'équation de Pell-Fermat (2.1) et (x_1, y_1) désigne sa solution minimale. La relation (2.5) sera utilisée à plusieurs reprises. Pour alléger l'écriture, nous la réécrivons comme suit :

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k. \tag{2.6}$$

Lemme 2.8.

1. *On a $x_1 > 1$ et $y_1 > 0$.*
2. *La suite $((x_1 + y_1\sqrt{d})^k)_{k\geqslant 0}$ est strictement croissante.*
3. *Si (x, y) est une solution à coordonnées strictement positives de l'équation de Pell-Fermat* (2.1)*, alors $x + y\sqrt{d} \geqslant x_1 + y_1\sqrt{d}$.*
4. *Si (x, y) est une solution de l'équation de Pell-Fermat* (2.1) *tel que $x + y\sqrt{d} > 1$, alors $x, y > 0$.*

Démonstration.

1. Comme (x_1, y_1) désigne la solution minimale de l'équation de Pell-Fermat (2.1), alors, d'après la définition 2.7 deux cas se présentent :
   — **Cas 1 :** $(x_1, y_1) = (p_{m-1}, q_{m-1})$. Ce cas se produit lorsque m est pair. D'où $m \geqslant 2$. Par suite $m - 1 \geqslant 1$. Comme $a_0 = \lfloor \sqrt{d} \rfloor \geqslant 1$, alors d'après la proposition 1.11, $p_{m-1} \geqslant p_1 > p_0$. Puisque selon la relation (1.27), $p_0 = a_0$, alors $p_{m-1} > 1$ et $y_1 = q_{m-1} > 0$.

— **Cas 2 :** $(x_1, y_1) = (p_{2m-1}, q_{2m-1})$. Ce cas se produit lorsque m est impair. Donc $m \geqslant 1$. Par suite $2m - 1 \geqslant 1$. En arrivant à cette étape il suffit de procéder comme dans le cas précédent pour arriver au résultat souhaité.

2. Comme $\sqrt{d} > 1$ et d'après la première assertion $y_1 > 0$, alors $x_1 + y_1\sqrt{d} > x_1$. En utilisant encore une fois la première assertion, nous obtenons $x_1 + y_1\sqrt{d} > 1$. Par conséquent, pour tout entier $k \geqslant 0$,

$$\frac{(x_1 + y_1\sqrt{d})^{k+1}}{(x_1 + y_1\sqrt{d})^k} > 1.$$

Ce qui signifie que la suite $((x_1 + y_1\sqrt{d})^k)_{k\geqslant 0}$ est strictement croissante.

3. D'après le corollaire 2.6, $y \geqslant y_1$ et $x \geqslant x_1$, alors $x + y\sqrt{d} \geqslant x_1 + y_1\sqrt{d}$.

4. On a par hypothèse (x, y) est un couple solution de l'équation de Pell-Fermat. Donc

$$\left(x - y\sqrt{d}\right)\left(x + y\sqrt{d}\right) = 1.$$

Autrement dit

$$x - y\sqrt{d} = \frac{1}{x + y\sqrt{d}}.$$

Et comme par hypothèse

$$1 < x + y\sqrt{d},$$

alors

$$0 < x - y\sqrt{d} < 1 < x + y\sqrt{d}.$$

Il en résulte de ces trois inégalités que $2x > 1$ et $2y\sqrt{d} > 0$. D'où $x > 0$ et $y > 0$.

□

Considérons les ensembles suivants :

$$S = \{x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}] \mid x^2 - dy^2 = 1\} \text{ et } S_+ = \{x + y\sqrt{d} \in S \mid x, y > 0\}.$$

Lemme 2.9. *Le plus petit élément de S_+ est $x_1 + y_1\sqrt{d}$.*

Démonstration. Comme (x_1, y_1) est la solution minimale de l'équation de Pell-Fermat (2.1), alors $x_1 + y_1\sqrt{d} \in S$. Et puisque d'après la première assertion du lemme 2.8, $x_1, y_1 > 0$, alors $x_1 + y_1\sqrt{d} \in S_+$. Soit maintenant $x + y\sqrt{d} \in S_+$. Donc (x, y) est un couple solution de l'équation de Pell-Fermat à coordonnées strictement positives. Donc, d'après la troisième assertion du lemme 2.8, $x + y\sqrt{d} \geqslant x_1 + y_1\sqrt{d}$. Par conséquent, $x_1 + y_1\sqrt{d}$ est le plus petit élément de S_+. □

Proposition 2.10. *Pour tout entier $k \geqslant 0$, (x_k, y_k) est un couple solution de l'équation de Pell-Fermat* (2.1)*. De plus, $(x_k, y_k) \in \mathbb{N}^* \times \mathbb{N}$.*

Démonstration.

— Considérons le $\mathbb{Q}$-automorphisme de corps $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ définie par $\sigma(x + y\sqrt{d}) = x - y\sqrt{d}$. Donc pour tout entier $k \geqslant 0$,

$$x_k - y_k\sqrt{d} = \sigma(x_k + y_k\sqrt{d}).$$

En utilisant la relation (2.6), nous obtenons :

$$x_k - y_k\sqrt{d} = \sigma((x_1 + y_1\sqrt{d})^k).$$

Puisque σ est un morphisme de corps, alors

$$\begin{aligned} x_k - y_k\sqrt{d} &= (\sigma(x_1 + y_1\sqrt{d}))^k \\ &= (x_1 - y_1\sqrt{d})^k. \end{aligned}$$

En tenant compte de cela et de la relation (2.6), nous obtenons :

$$\begin{aligned} (x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) &= (x_1 + y_1\sqrt{d})^k(x_1 - y_1\sqrt{d})^k \\ &= ((x_1 + y_1\sqrt{d})(x_1 - y_1\sqrt{d}))^k \\ &= \left(x_1^2 - dy_1^2\right)^k. \end{aligned}$$

Comme (x_1, y_1) désigne la solution minimale de l'équation de Pell-Fermat (2.1), alors

$$(x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) = 1.$$

Par conséquent, pour tout entier $k \geqslant 0$, (x_k, y_k) est un couple solution de l'équation de Pell-Fermat (2.1).

— Pour finir, montrons que pour tout entier $k \geqslant 0$, $(x_k, y_k) \in \mathbb{N} \times \mathbb{N}^*$. Commençons par $k = 0$. Dans ce cas la relation (2.6) nous permet de déduire que $(x_0, y_0) = (1, 0)$, ce qui est évidemment dans $\mathbb{N}^* \times \mathbb{N}$. Supposons maintenant que $k \geqslant 1$. Comme d'après la troisième assertion du lemme 2.8, la suite $((x_1 + y_1\sqrt{d})^k)_{k\geqslant 0}$ est strictement croissante, alors

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k \geqslant x_1 + y_1\sqrt{d}.$$

En revenant à la démonstration de la seconde assertion du lemme 2.8, nous trouvons que $x_1 + y_1\sqrt{d} > 1$. Par conséquent, pour tout $k \geqslant 1$, $x_k + y_k\sqrt{d} > 1$. Donc, comme en vertu de l'assertion précédente, pour tout entier $k \geqslant 0$, (x_k, y_k) est une solution de l'équation de Pell-Fermat (2.1), alors d'après la dernière assertion du lemme 2.8, pour tout entier $k \geqslant 1$, $x_k, y_k > 0$.

□

Proposition 2.11. *Soit (x, y) une solution à coordonnées positives de l'équation de Pell-Fermat (2.1). Alors il existe un entier $k \geqslant 0$ tel que $(x, y) = (x_k, y_k)$.*

Démonstration.

— Si $(x, y) = (1, 0)$, alors d'après la relation (2.6), $(x, y) = (x_0, y_0)$.

— Supposons que (x, y) est une solution non-triviale. D'après la troisième assertion du lemme 2.8, $x + y\sqrt{d} \geqslant x_1 + y_1\sqrt{d}$. Comme d'après le même lemme, la suite $((x_1 + y_1\sqrt{d})^k)_{k\geqslant 0}$ est strictement croissante, alors il existe un entier $k \geqslant 1$, tel que

$$(x_1 + y_1\sqrt{d})^k \leqslant x + y\sqrt{d} < (x_1 + y_1\sqrt{d})^{k+1}.$$

En utilisant la relation (2.6), nous obtenons ce qui suit

$$x_k + y_k\sqrt{d} \leqslant x + y\sqrt{d} < (x_k + y_k\sqrt{d})(x_1 + y_1\sqrt{d}).$$

En multipliant maintenant par $x_k - y_k\sqrt{d}$ et en tenant compte de la proposition 2.10, selon laquelle pour tout entier $k \geqslant 0$, (x_k, y_k) est solution de l'équation de Pell-Fermat (2.1), nous obtenons

$$1 \leqslant (x + y\sqrt{d})(x_k - y_k\sqrt{d}) < x_1 + y_1\sqrt{d}. \tag{2.7}$$

Posons

$$e + f\sqrt{d} = (x + y\sqrt{d})(x_k - y_k\sqrt{d}). \tag{2.8}$$

Donc,

$$e^2 - df^2 = (x + y\sqrt{d})(x_k - y_k\sqrt{d})(x - y\sqrt{d})(x_k + y_k\sqrt{d}).$$

Comme par hypothèse (x, y) est une solution de l'équation de Pell-Fermat, et (x_k, y_k) l'est également en vertu de la proposition 2.10, alors $e^2 - df^2 = 1$. Autrement dit (e, f) est un couple solution de l'équation de Pell-Fermat. D'où $e + f\sqrt{d} \in S$.
Supposons maintenant que $e + f\sqrt{d} \neq 1$. Donc, d'après la relation (2.7), $e + f\sqrt{d} > 1$. Comme (e, f) est une solution de l'équation de Pell-Fermat, alors selon la dernière assertion du lemme 2.8, $e, f > 0$. Ainsi, puisque $e + f\sqrt{d} \in S$, alors $e + f\sqrt{d} \in S_+$. Par conséquent, d'après le lemme 2.9, $e + f\sqrt{d} \geqslant x_1 + y_1\sqrt{d}$. Ce qui contredit la relation (2.7). Donc notre supposition selon laquelle $e + f\sqrt{d} \neq 1$ est fausse. Par conséquent, $e + f\sqrt{d} = 1$. En utilisant la relation (2.8), nous obtenons

$$x + y\sqrt{d} = \frac{1}{x_k - y_k\sqrt{d}} = x_k + y_k\sqrt{d}.$$

D'où $x = x_k$ et $y = y_k$. Ce qui termine la preuve.

□

Il découle des propositions 2.10 et 2.11 le corollaire suivant :

Corollaire 2.12. *L'ensemble des solutions à coordonnées positives de l'équation de Pell-Fermat* (2.1) *est composé des couples* (x_k, y_k) *donnés par la relation*

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k, \qquad k \in \mathbb{N}.$$

Les exemples suivant illustrent le corollaire 2.12.

Exemple 2.13. *Nous allons résoudre l'équation de Pell-Fermat pour* $d = 11$. *D'après l'exemple 1.47, le développement en fraction continue de* $\sqrt{17}$ *est de la forme* $\sqrt{17} = \left[4, \overline{8}\right]$, *la période* $m = 1$ *et* $(p_1, q_1) = (33, 8)$. *Alors selon la définition 2.7,* (p_1, q_1) *est la solution minimale de l'équation de Pell-Fermat*

$$u^2 - 17v^2 = 1.$$

Pour trouver toutes les autres solutions à coordonnées positives, nous appliquons le corollaire 2.12 selon lequel pour tout entier $k \geqslant 0$,

$$x_k + y_k\sqrt{17} = \left(x_1 + y_1\sqrt{17}\right)^k,$$

où $(x_1, y_1) = (p_1, q_1) = (33, 8)$. *Par exemple, pour trouver la solution* (x_2, y_2), *nous remplaçons* k *par* 2, *ce qui nous donne :*

$$x_2 + y_2\sqrt{17} = (33 + 8\sqrt{17})^2 = 2177 + 528\sqrt{17}.$$

Par conséquent, $(x_2, y_2) = (2177, 528)$.

Exemple 2.14. *Nous allons résoudre ici l'équation* $u^2 - 6083v^2 = 1$. *D'après l'exemple 1.48, le développement en fraction continue de* $\sqrt{6083}$ *est*

$$\sqrt{6083} = \left[77, \overline{1, 154}\right].$$

Donc il est périodique de période $m = 2$. *Alors selon la définition 2.7,* $(p_1, q_1) = (78, 1)$ *est la solution minimale de l'équation de Pell-Fermat*

$$u^2 - 6083v^2 = 1.$$

Pour trouver toutes les solutions à coordonnées positives, il suffit d'appliquer le corollaire 2.12 selon lequel pour tout entier $k \geqslant 0$,

$$x_k + y_k\sqrt{6083} = \left(x_1 + y_1\sqrt{6083}\right)^k,$$

où $(x_1, y_1) = (p_1, q_1) = (78, 1)$.

2.2 Récurrences dans la suite des solutions de l'équation de Pell-Fermat

Dans cette section, nous nous intéressons aux suites $(x_k)_{k\geqslant 0}$ et $(y_k)_{k\geqslant 0}$, où pour tout entier $k \geqslant 0$, (x_k, y_k) représente d'après le corollaire 2.12 une solution à coordonnées positives

de l'équation de Pell-Fermat (2.1). Nous verrons par exemple que ces dernières vérifient, pour tout entier $k \geqslant 0$, les relations suivantes :

$$x_{k+2} = 2x_1x_{k+1} - x_k, \quad y_{k+2} = 2x_1y_{k+1} - y_k \quad et \quad x_{2k} = 2x_k^2 - 1,$$

où (x_1, y_1) représente la solution minimale de l'équation de Pell-Fermat (2.1). Ces relations constituent l'un des résultats principaux de cette section, et joueront un rôle important dans le dernier chapitre lors de l'étude de l'équation diophantienne

$$(a^n - 1)(b^m - 1) = x^2.$$

Nous donnerons aussi l'expression du terme général pour chacune de ces suites. Nous commençons cette section par la proposition suivante.

Proposition 2.15. *Soient r et s deux entiers positifs. Nous avons :*

1. $x_{r+s} = x_rx_s + dy_ry_s$.
2. $y_{r+s} = x_ry_s + x_sy_r$.

Démonstration. D'après le corollaire 2.12, pour tout entier $k \geqslant 0$, x_k et y_k s'obtiennent à partir de la formule (2.6) :

$$x_k + y_k\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^k.$$

Donc,

$$\begin{aligned} x_{r+s} + y_{r+s}\sqrt{d} &= \left(x_1 + y_1\sqrt{d}\right)^{r+s} \\ &= \left(x_1 + y_1\sqrt{d}\right)^r \left(x_1 + y_1\sqrt{d}\right)^s. \end{aligned}$$

En utilisant à nouveau la relation (2.6), nous obtenons :

$$x_{r+s} + y_{r+s}\sqrt{d} = \left(x_r + y_r\sqrt{d}\right)\left(x_s + y_s\sqrt{d}\right).$$

Par suite,

$$x_{r+s} + y_{r+s}\sqrt{d} = (x_rx_s + dy_ry_s) + (x_ry_s + x_sy_r)\sqrt{d}.$$

Par conséquent,

$$x_{r+s} = x_rx_s + dy_ry_s \text{ et } y_{r+s} = x_ry_s + x_sy_r.$$

Ce qui termine la preuve. □

Le corollaire suivant découle directement de la proposition précédente.

Corollaire 2.16. *Pour tout entier $k \geqslant 0$,*

1. $x_{2k} = 2x_k^2 - 1$.
2. $y_{2k} = 2x_ky_k$.

3. $x_{k+1} = x_k x_1 + d y_k y_1$.

4. $y_{k+1} = x_k y_1 + x_1 y_k$.

5. $x_{k+2} = 2x_1 x_{k+1} - x_k$.

6. $y_{k+2} = 2x_1 y_{k+1} - y_k$.

Démonstration.

— Soit k un entier naturel et montrons que $x_{2k} = 2x_k^2 - 1$. D'après la première assertion de la proposition 2.15,

$$x_{2k} = x_k^2 + d y_k^2.$$

Comme (x_k, y_k) est solution de l'équation de Pell-Fermat (2.1), alors $d y_k^2 = x_k^2 - 1$. Par conséquent,

$$x_{2k} = 2x_k^2 - 1.$$

— La deuxième et la quatrième formule s'obtiennent en remplaçant une fois r et s par k, et une fois (r, s) par $(k, 1)$ dans l'égalité donnée par l'assertion (2) de la proposition 2.15. Quant à la troisième formule, elle s'obtient en remplaçant (r, s) par $(k, 1)$ dans l'égalité donnée par l'assertion (1) de la proposition 2.15.

— Passons à la preuve de la cinquième assertion. D'après la première assertion de la proposition 2.15,

$$x_{k+2} = x_k x_2 + d y_k y_2.$$

Comme, d'après la première et la seconde assertion du présent corollaire,

$$x_2 = 2x_1^2 - 1 \text{ et } y_2 = 2x_1 y_1, \tag{2.9}$$

alors,

$$x_{k+2} = x_k \left(2x_1^2 - 1\right) + d y_k \left(2x_1 y_1\right).$$

Par suite,

$$x_{k+2} = 2x_1 \left(x_k x_1 + d y_k y_1\right) - x_k.$$

En utilisant la troisième assertion de ce corollaire, nous obtenons

$$x_{k+2} = 2x_1 x_{k+1} - x_k.$$

— Enfin, montrons que pour tout entier $k \geqslant 0$, $y_{k+2} = 2x_1 y_{k+1} - y_k$. D'après la deuxième assertion de la proposition 2.15,

$$y_{k+2} = x_k y_2 + x_2 y_k.$$

En utilisant maintenant la relation (2.9), nous obtenons

$$y_{k+2} = x_k(2x_1 y_1) + (2x_1^2 - 1) y_k.$$

Par suite,

$$y_{k+2} = 2x_1 (x_k y_1 + x_1 y_k) - y_k.$$

Comme d'après l'assertion (4) de ce corollaire, $y_{k+1} = x_k y_1 + x_1 y_k$, alors

$$y_{k+2} = 2x_1 y_{k+1} - y_k.$$

□

La proposition suivante est très importante, car elle a été essentielle pour prouver un nouveau résultat [1], que nous verrons dans le chapitre suivant, à savoir le corollaire 2.31 .

Proposition 2.17. *Soient $i \in \mathbb{N}^*$, et k et m deux entiers naturels. Nous avons :*

1. $x_{im} = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2j} x_i^{m-2j} \left(x_i^2 - 1\right)$.
2. $y_{im} = y_i \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x_i^{m-2j-1} \left(x_i^2 - 1\right)^j$.
3. *Si $i \mid k$, alors $y_i \mid y_k$.*
4. $x_k = \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} x_1^{k-2j} \left(x_1^2 - 1\right)^j$.
5. $y_k = y_1 \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} \binom{k}{2j+1} x_1^{k-2j-1} \left(x_1^2 - 1\right)^j$.

Démonstration.

— Commençons par prouver les deux premières assertions. Rappelons que pour tout entier $k \geqslant 0$, x_k et y_k s'obtiennent à partir de la relation (2.6) :

$$x_k + y_k\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^k.$$

Donc,

$$x_{im} + y_{im}\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^{im}.$$

Par suite,

$$x_{im} + y_{im}\sqrt{d} = \left(\left(x_1 + y_1\sqrt{d}\right)^i\right)^m.$$

En utilisant à nouveau la relation (2.6), nous obtenons :

$$x_{im} + y_{im}\sqrt{d} = \left(x_i + y_i\sqrt{d}\right)^m.$$

En appliquant le formule du binôme de Newton au membre droit de cette égalité, nous obtenons :

$$x_{im} + y_{im}\sqrt{d} = \sum_{j=0}^{m} \binom{m}{j} x_i^{m-j} \left(y_i\sqrt{d}\right)^j.$$

En séparant les termes pairs et impairs du membre droit de l'égalité ci-dessus, nous obtenons :

$$x_{im} + y_{im}\sqrt{d} = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2j} x_i^{m-2j} \left(y_i\sqrt{d}\right)^{2j} + \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x_i^{m-2j-1} \left(y_i\sqrt{d}\right)^{2j+1}.$$

Comme (x_i, y_i) est solution de l'équation de Pell-Fermat (2.1), alors $dy_i^2 = x_i^2 - 1$. Par conséquent,

$$x_{im}+y_{im}\sqrt{d} = \left(\sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2j} x_i^{m-2j} \left(x_i^2-1\right)^j \right) + \left(y_i \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x_i^{m-2j-1} \left(x_i^2-1\right)^j \right) \sqrt{d}.$$

D'où,

$$x_{im} = \sum_{j=0}^{\lfloor \frac{m}{2} \rfloor} \binom{m}{2j} x_i^{m-2j} \left(x_i^2-1\right)^j$$

et

$$y_{im} = y_i \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x_i^{m-2j-1} (x_i^2-1)^j.$$

— Passons à la preuve de la troisième assertion. Supposons que $i \mid k$. Alors il existe un entier naturel m tel que $k = im$. D'après la seconde assertion du présent corollaire,

$$y_k = y_{im} = y_i \sum_{j=0}^{\lfloor \frac{m-1}{2} \rfloor} \binom{m}{2j+1} x_i^{m-2j-1} \left(x_i^2-1\right)^j.$$

Comme x_i est un entier naturel, alors $y_i \mid y_k$.

— Les deux dernières égalités s'obtiennent à partir des deux premières.

□

En plus de la proposition précédente, nous ferons également appel à ce résultat lors de la démonstration du corollaire 2.31.

Lemme 2.18. *Pour tout $k \geqslant 0$, les suites $(x_k)_{k\geqslant 0}$ et $(y_k)_{k\geqslant 0}$ sont strictement croissantes.*

Démonstration. D'après la première assertion du lemme 2.8,

$$x_1 > 1 = x_0 \text{ et } y_1 > 0 = y_0,$$

où (x_0, y_0) est la solution triviale de l'équation de Pell-Fermat. Montrons maintenant que pour tout entier $k \geqslant 1$, $x_{k+1} > x_k$ et $y_{k+1} > y_k$. Comme $x_1 > 1$ et x_k, y_k, d et y_1 sont des entiers strictement positifs, alors

$$x_k x_1 + d y_k y_1 > x_k \quad \text{et} \quad x_k y_1 + x_1 y_k > y_k.$$

En utilisant les assertions (3) et (4) du corollaire 2.16, nous obtenons $x_{k+1} > x_k$ et $y_{k+1} > y_k$. Par conséquent, les suites $(x_k)_{k\geqslant 0}$ et $(y_k)_{k\geqslant 0}$ sont strictement croissantes. □

Nous clôturons cette section par le résultat suivant, dont l'intérêt se verra lors de la démonstration du théorème 3.13 du dernier chapitre.

Lemme 2.19.

1. *S'il existe un entier $\ell \geqslant 1$ tel que $x_\ell = 78$ alors pour tout entier k*

$$x_{2k} \equiv (-1)^k \pmod{156} \quad \textit{et} \quad x_{2k+1} \equiv 78 \pmod{156}.$$

Démonstration. Comme $(78, y_\ell)$ est solution de l'équation de Pell-Fermat (2.1), alors

$$dy_\ell^2 = 78^2 - 1 = 6083 = 7 \times 11 \times 79.$$

Par conséquent $d = 6083$. D'après l'exemple 2.14 $(x_1, y_1) = (78, 1)$ est la solution minimale de l'équation de Pell-Fermat $x^2 - 6083y^2 = 1$. Commençons par montrer par récurrence que pour tout entier $k \geqslant 0$, $x_{2k} \equiv (-1)^k \pmod{156}$.

— Comme $x_0 = 1$, alors la formule est vérifiée pour $k = 0$.

— Fixons $k \geqslant 0$. Supposons que $x_{2k} \equiv (-1)^k \pmod{156}$, et montrons que

$$x_{2(k+1)} \equiv (-1)^{k+1} \pmod{156}.$$

Comme $x_1 = 78$, donc en utilisant la cinquième assertion du corollaire 2.16, nous obtenons

$$x_{2(k+1)} = 156x_{2k+1} - x_{2k}.$$

Donc,

$$x_{2(k+1)} = -x_{2k} \pmod{156}.$$

L'hypothèse de récurrence nous permet de déduire que

$$x_{2(k+1)} \equiv (-1)^{k+1} \pmod{156}.$$

Pour finir, montrons que pour tout entier $k \geqslant 0$, $x_{2k+1} \equiv 78 \pmod{156}$.

— Comme $x_1 = 78$, alors la formule est vérifiée pour $k = 0$.

— Fixons $k \geqslant 0$. Supposons que $x_{2k+1} \equiv 78 \pmod{156}$, et montrons que

$$x_{2(k+1)+1} \equiv 78 \pmod{156}.$$

Comme $x_1 = 78$, alors en utilisant à nouveau la cinquième assertion du corollaire 2.16, nous obtenons :

$$x_{2k+3} = 156x_{2k+2} - x_{2k+1}.$$

Donc

$$x_{2k+3} \equiv -x_{2k+1} \pmod{156}.$$

L'hypothèse de récurrence nous permet de déduire que

$$x_{2k+3} \equiv -78 \pmod{156} \equiv 78 \pmod{156}.$$

Conclusion : Ainsi, par le principe de récurrence, pour tout entier $k \geqslant 0$, nous avons $x_{2k} \equiv (-1)^k \pmod{156}$ et $x_{2k+1} \equiv 78 \pmod{156}$.

□

2.3 Équation de Pell-Fermat et polynômes de Tchebychev

Dans cette section, nous donnons le lien entre les solutions à coordonnées positives de l'équation de Pell-Fermat et les polynômes de Tchebychev de première et de seconde espèce, notés respectivement T_k et U_k, où $k \in \mathbb{N}$. Ces derniers peuvent être définis par

$$T_0(X) = 1,\ T_1(X) = X,\ U_0(X) = 1,\ U_1(X) = 2X, \tag{2.10}$$

et pour tout entier $k \geqslant 0$,

$$T_{k+2}(X) = 2XT_{k+1}(X) - T_k(X) \quad \text{et} \quad U_{k+2}(X) = 2XU_{k+1}(X) - U_k(X). \tag{2.11}$$

Par exemple,

$$T_2(X) = 2X^2 - 1 \text{ et } U_2(X) = 4X^2 - 1.$$

Théorème 2.20 ([10])**.**

1. *Pour tout $k \in \mathbb{N}$, $x_k = T_k(x_1)$.*
2. *Pour tout entier $k \geqslant 1$, $y_k = y_1U_{k-1}(x_1)$.*

Démonstration. Commençons par prouver que pour tout entier $k \geqslant 0$, $x_k = T_k(x_1)$.

— En utilisant la relation (2.10), on obtient : $x_0 = 1 = T_0(x_1)$ et $x_1 = T_1(x_1)$.

— Fixons $k \geqslant 1$. Supposons que pour tout entier n, $1 \leqslant n \leqslant k$, $x_n = T_n(x_1)$, et montrons que $x_{k+1} = T_{k+1}(x_1)$. D'après la cinquième assertion du corollaire 2.16,

$$x_{k+1} = 2x_1x_k - x_{k-1}.$$

En utilisant l'hypothèse de récurrence, nous obtenons

$$x_{k+1} = 2x_1T_k(x_1) - T_{k-1}(x_1).$$

En utilisant la relation (2.11), on obtient $x_{k+1} = T_{k+1}(x_1)$.

Conclusion : Par le principe de récurrence, pour tout entier $k \geqslant 1$, $x_k = T_k(x_1)$.
Pour finir, prouvons que pour tout entier $k \geqslant 1$, $y_k = y_1 U_{k-1}(x_1)$.

— En utilisant la relation (2.10), nous pouvons facilement vérifier que $y_1 = y_1 U_0(x_1)$. En utilisant la formule donnée par la seconde assertion du corollaire 2.16 et la relation (2.10) on obtient : $y_2 = y_1 U_1(x_1)$. Ainsi, la relation est vérifiée pour $k = 1$ et 2.

— Fixons $k \geqslant 2$. Supposons que pour tout entier n, $1 \leqslant n \leqslant k$, $y_n = y_1 U_{n-1}(x_1)$ et montrons que $y_{k+1} = y_1 U_k(x_1)$. D'après la dernière assertion du corollaire 2.16,

$$y_{k+1} = 2x_1 y_k - y_{k-1}.$$

En utilisant l'hypothèse de récurrence, nous obtenons :

$$\begin{aligned} y_{k+1} &= 2x_1 y_1 U_{k-1}(x_1) - y_1 U_{k-2}(x_1). \\ &= y_1 \left(2x_1 U_{k-1}(x_1) - U_{k-2}(x_1)\right). \end{aligned}$$

En utilisant la relation (2.11), nous trouvons que $y_{k+1} = y_1 U_k(x_1)$.
Conclusion : Par le principe de récurrence, pour tout entier $k \geqslant 1$, $y_k = y_1 U_{k-1}(x_1)$. □

2.4 Divisibilité et congruences

Soit p un nombre premier. Le plus petit entier h tel que $p \mid x_h$ est dit *indice de divisibilité* de p dans $(x_k)_{k\geqslant 0}$, et il est noté $h(p)$. S'il n'existe aucun entier $k \geqslant 0$ tel que x_k soit divisible par p, alors $h(p) = +\infty$. En 2010, Lan et Szalay [11] se sont intéressés à l'étude de l'indice de divisibilité dans le cas où $p \in \{2, 3, 5\}$. Ils ont prouvé qu'il est soit égal $+\infty$ soit égal à 1. Ils ont remarqué que cela n'est pas valable pour le reste des nombres premiers. Par exemple, pour l'équation de Pell-Fermat $x^2 - 3y^2 = 1$, $(x_1, y_1) = (2, 1)$ et $(x_2, y_2) = (7, 4)$. Donc $h(7) = 2$. Dans [1], nous avons amélioré le résultat de Lan et Szalay [11], en donnant la valeur de $h(p)$, pour tout nombre premier impair p. Cela constitue l'un des principaux résultats de cette section. La démonstration repose sur l'expression du terme général de la suite $(\overline{x_k})_{k\geqslant 0}$, où $\overline{x_k}$ représente la classe d'équivalence de x_k modulo p. Nous allons présenter des résultats concernant cette dernière qui seront utiles dans le chapitre suivant, lequel est consacré à l'étude de l'équation diophantienne $(a^n - 1)(b^m - 1) = x^2$.

Nous débutons cette section par donner la définition d'une suite récurrente linéaire.

Définition 2.21. *Soit $(u_k)_{k\in\mathbb{N}}$ une suite à valeur dans un corps commutatif K vérifiant pour tout $k \in \mathbb{N}$*

$$u_{k+h} = a_{h-1}u_{k+h-1} + a_{h-2}u_{k+h-2} + \cdots + a_0 u_k.$$

où $h \in \mathbb{N}^*$ et $a_i \in K$. Alors la suite $(u_k)_{k\in\mathbb{N}}$ est dite récurrente linéaire et le polynôme $P(X) = X^{k+h} - a_{h-1}X^{k+h-1} - a_{h-2}X^{k+h-2} - \cdots - a_0 \in K[x]$ est appelé polynôme caractéristique associé à la suite $(u_k)_{k\in\mathbb{N}}$.

Exemple 2.22. *Les suites $(x_k)_{k\geqslant 0}$ et $(y_k)_{k\geqslant 0}$, où pour tout $k \geqslant 0$, (x_k, y_k) représente un*

couple solution de l'équation de Pell-Fermat (2.1) *sont d'après la cinquième et la sixième assertion du corollaire 2.16 des suites récurrentes linéaires.*

Exemple 2.23. *Soit p un nombre premier. Considérons la suite $(\overline{x_k})_{k\geqslant 0}$, où pour tout entier $k \geqslant 0$, $\overline{x_k}$ représente la classe d'équivalence de x_k modulo p. Comme, d'après la cinquième assertion de la proposition 2.16,*

$$x_{k+2} = 2x_1x_{k+1} - x_k,$$

alors

$$\overline{x_{k+2}} = 2\overline{x_1}\ \overline{x_{k+1}} - \overline{x_k}.$$

Par conséquent, la suite $(\overline{x_k})_{k\geqslant 0}$ est une suite récurrente linéaire.

Proposition 2.24. *Soient p un nombre premier et $(u_k)_{k\geqslant 0}$ une suite à valeur dans $\mathbb{F}_p$ tels que $u_0 = 1$, et pour tout entier $k \geqslant 0$, $u_{k+2} = 2u_1u_{k+1} - u_k$. Alors, pour tout entier $k \geqslant 0$,*

$$u_k = \begin{cases} \dfrac{\alpha^k + \alpha^{-k}}{2} \ \textit{si } p \neq 2 \\ 1 + k + ku_1 \ \textit{si } p = 2 \end{cases}$$

où α est une racine du polynôme $P(X) = X^2 - 2u_1X + 1$ dans une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$.

Démonstration. Considérons la série génératrice associée à la suite $(u_k)_{k\in\mathbb{N}}$, qui est, rappellons le la série formelle

$$\sum_{k\geqslant 0} u_kX^k.$$

— On se propose de prouver que

$$\sum_{k\geqslant 0} u_kX^k = \frac{1 - u_1X}{P(X)}.$$

$$\begin{aligned} P(X)\sum_{k\geqslant 0} u_kX^k &= (X^2 - 2u_1X + 1)\sum_{k\geqslant 0} u_kX^k \\ &= \sum_{k\geqslant 0} u_kX^{k+2} - \sum_{k\geqslant 0} 2u_1u_kX^{k+1} + \sum_{k\geqslant 0} u_kX^k \\ &= \sum_{k\geqslant 0} u_kX^{k+2} - 2u_1u_0X - \sum_{k\geqslant 1} 2u_1u_kX^{k+1} + u_0 + u_1X + \sum_{k\geqslant 2} u_kX^k \\ &= -2u_1u_0X + u_0 + u_1X + \sum_{k\geqslant 0}(u_{k+2} - 2u_1u_{k+1} + u_k)X^{k+2}. \end{aligned}$$

Puisque par hypothèse $u_0 = 1$ et pour tout $k \geqslant 0$, $u_{k+2} = 2u_1u_{k+1} - u_k$, alors

$$P(X)\sum_{k\geqslant 0} u_kX^k = 1 - u_1X.$$

Par conséquent,

$$\sum_{k\geqslant 0} u_k X^k = \frac{1-u_1 X}{P(X)}. \tag{2.12}$$

— Montrons maintenant que pour tout entier $k \geqslant 0$,

$$u_k = \begin{cases} \dfrac{\alpha^k + \alpha^{-k}}{2} \text{ si } p \neq 2 \\ 1 + k + k u_1 \text{ si } p = 2. \end{cases}$$

Soit α une racine de P dans une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$. Comme

$$P(X) = X^2 - 2u_1 X + 1,$$

alors α^{-1} est l'autre racine de P, $\alpha + \alpha^{-1} = 2u_1$ et $P(X) = (X-\alpha)(X-\alpha^{-1})$. Ce qui nous permet de réécrire (2.12) comme suit :

$$\sum_{k\geqslant 0} u_k X^k = \frac{1-u_1 X}{(X-\alpha)(X-\alpha^{-1})}. \tag{2.13}$$

Occupons nous du membre droit de l'égalité ci-dessus. Nous avons trois cas à traiter :

— **cas 1.1** : $p \neq 2$ et $\alpha \neq \alpha^{-1}$. Dans ce cas,

$$\frac{1-u_1 X}{(X-\alpha)(X-\alpha^{-1})} = \frac{\frac{1-u_1\alpha}{\alpha-\alpha^{-1}}}{X-\alpha} + \frac{\frac{1-u_1\alpha^{-1}}{\alpha^{-1}-\alpha}}{X-\alpha^{-1}}.$$

En utilisant le fait que $u_1 = \dfrac{\alpha+\alpha^{-1}}{2}$, $\alpha - \alpha^{-1} = \alpha - \frac{1}{\alpha}$ et $\alpha^{-1} - \alpha = \alpha^{-1} - \frac{1}{\alpha^{-1}}$, nous obtenons :

$$\sum_{k\geqslant 0} u_k X^k = \frac{\frac{-\alpha}{2}}{X-\alpha} + \frac{\frac{-\alpha^{-1}}{2}}{X-\alpha^{-1}}.$$

Par suite,

$$\begin{aligned} \sum_{k\geqslant 0} u_k X^k &= \frac{\frac{\alpha}{2}}{\alpha\left(1-\frac{X}{\alpha}\right)} + \frac{\frac{\alpha^{-1}}{2}}{\alpha^{-1}\left(1-\frac{X}{\alpha^{-1}}\right)} \\ &= \frac{1}{2}\left(\frac{1}{1-\frac{X}{\alpha}} + \frac{1}{1-\frac{X}{\alpha^{-1}}}\right) \\ &= \frac{1}{2}\left(\sum_{k\geqslant 0}\left(\frac{X}{\alpha}\right)^k + \sum_{k\geqslant 0}\left(\frac{X}{\alpha^{-1}}\right)^k\right) \\ &= \sum_{k\geqslant 0} \frac{\alpha^k + \alpha^{-k}}{2} X^k. \end{aligned}$$

Par conséquent, pour tout entier $k \geqslant 0$,

$$u_k = \frac{\alpha^k + \alpha^{-k}}{2}.$$

— **Cas 1.2** : $p \neq 2$ et $\alpha = \alpha^{-1}$. Dans ce cas (2.13) se réécrit comme suit :

$$\sum_{k\geqslant 0} u_k X^k = \frac{1-u_1 X}{(X-\alpha)^2}. \tag{2.14}$$

Rappelons que $(X-\alpha)^2 = P(X)$ et $P(X) = X^2 - 2u_1 X + 1$. Donc $\alpha = u_1$ et $\alpha^2 = 1$. Par conséquent, en utilisant (2.14) nous obtenons :

$$\sum_{k\geqslant 0} u_k X^k = \frac{1-\alpha X}{(1-\alpha X)^2} = \frac{1}{1-\alpha X} = \sum_{k\geqslant 0} \alpha^k X^k.$$

Par conséquent, pour tout entier $k \geqslant 0$,

$$u_k = \alpha^k = \frac{\alpha^k + \alpha^{-k}}{2}.$$

— **Cas 2 :** $p = 2$. Dans ce cas, $P(X) = (X-1)^2$, c'est-à-dire $\alpha = \alpha^{-1} = 1$. Par conséquent, (2.13) devient comme suit :

$$\begin{aligned}
\sum_{k\geqslant 0} u_k X^k = \frac{1-u_1 X}{(X-1)^2} &= (1-u_1 X)\left(\frac{1}{1-X}\right)' \\
&= (1-u_1 X)\left(\sum_{k\geqslant 0} X^k\right)' = (1-u_1 X)\sum_{k\geqslant 1} k X^{k-1} \\
&= \sum_{k\geqslant 1} k X^{k-1} + \sum_{k\geqslant 1} k u_1 X^k \\
&= \sum_{k\geqslant 0} (k+1) X^k + \sum_{k\geqslant 1} k u_1 X^k
\end{aligned}$$

En remarquant que

$$\sum_{k\geqslant 1} k u_1 X^k = \sum_{k\geqslant 0} k u_1 X^k,$$

on obtient

$$\sum_{k\geqslant 0} u_k X^k = \sum_{k\geqslant 0} (k+1+k u_1) X^k.$$

En d'autres termes, pour tout $k \in \mathbb{N}$, $u_k = k+1+k u_1$.

□

Soit p un nombre premier. Pour tout entier $k \geqslant 0$, posons $u_k = \overline{x_k}$, où $\overline{x_k}$ représente la classe d'équivalence de x_k modulo p. D'après l'exemple 2.23, pour tout entier $k \geqslant 0$, $u_{k+2} = 2u_1 u_{k+1} - u_k$. Comme $u_0 = \overline{x_0} = 1$, alors d'après la proposition 2.24, l'expression du

terme générale de la suite $(u_k)_{k\geqslant 0}$ est donné par

$$u_k = \begin{cases} \dfrac{\alpha^k + \alpha^{-k}}{2} \text{ si } p \neq 2 \\ 1 + k + ku_1 \text{ si } p = 2 \end{cases} \tag{2.15}$$

où α désigne l'une des racines du polynôme $P(X) = X^2 - 2u_1X + 1$ dans une clôture algébrique $\overline{\mathbb{F}_p}$ de $\mathbb{F}_p$. Dans toute la suite q désigne l'ordre de α dans le groupe multiplicatif $\left(\overline{\mathbb{F}_p}\right)^*$.

Lemme 2.25 ([1]). *Soit p un nombre premier impair. S'il existe un entier $s \geqslant 1$ tel que $u_s = 0$, alors q est divisible par 4.*

Démonstration. Commençons par prouver que $\text{ord}(\alpha^s) = 4$. Comme $u_s = 0$ et p est un nombre premier impair, alors d'après la relation (2.15),

$$u_s = \frac{\alpha^s + \alpha^{-s}}{2} = 0$$

En multipliant par $2\alpha^s$, nous obtenons $(\alpha^s)^2 + 1 = 0$. Par suite $(\alpha^s)^2 = -1$. D'où, $(\alpha^s)^4 = 1$. Il en résulte que $\text{ord}\,(\alpha^s) \mid 4$. Mais comme $(\alpha^s)^2 = -1$, qui est différent de 1 puisque p est supposé impair. Alors $ord\,(\alpha^s) = 4$.
Vu que α^s est un élément d'ordre 4 du sous-groupe de $\overline{\mathbb{F}_p}^*$ engendré par α, alors $4 \mid \text{ord}(\alpha) = q$. Ainsi la preuve est achevée. □

Définition 2.26. *Soit p un nombre premier. Le plus petit entier naturel h tel que $p \mid x_h$ est appelé indice de divisibilité de p dans $(x_k)_{k\geqslant 0}$. Il est noté $h(p)$. Si pour tout $k \geqslant 0$, $p \nmid x_k$ alors $h\,(p) = +\infty$.*

Rappelons le résultat donné par Lan et Szaly [11] en 2010.

Lemme 2.27 ([11]). *Si $p \in \{2, 3, 5\}$, alors $h\,(p) = 1$ ou bien $h\,(p) = +\infty$.*

Comme mentionné dans l'introduction de ce chapitre, nous avons élargi ce résultat en traitant le cas de tous les nombres premiers impairs. Ci-dessous l'énoncé de notre résultat.

Théorème 2.28 ([1]). *Si p est un nombre premier impair, alors $h\,(p) = +\infty$ ou $4h\,(p) = q = \text{ord}(\alpha)$.*

Démonstration. Posons $h\,(p) = h$, supposons que h est fini et montrons que $4h = q$. D'après le lemme 2.25, q est divisible par 4. Montrons que $h = \frac{q}{4}$. Cela revient à prouver que :

1. $u_{\frac{q}{4}} = 0$.
2. L'entier $\frac{q}{4}$ est le plus petit indice produisant un terme nul.

Commençons par le premier point. En utilisant la relation (2.15), nous obtenons :

$$\begin{aligned} u_{\frac{q}{4}} &= \frac{\alpha^{\frac{q}{4}} + \alpha^{\frac{-q}{4}}}{2} \\ &= \frac{1}{2}\alpha^{\frac{-q}{4}}\left(\alpha^{\frac{q}{2}} + 1\right) \end{aligned}$$

Rappelons que $q = \operatorname{ord}(\alpha)$, et donc $\alpha^q = \left(\alpha^{\frac{q}{2}}\right)^2 = 1$. Comme $\frac{q}{2} < q$, alors $\alpha^{\frac{q}{2}} = -1$. Par conséquent, $u_{\frac{q}{4}} = 0$.
Passons au second point. Supposons qu'il existe un entier $m \geqslant 1$ tel que $u_m = 0$. Donc, d'après la relation (2.15), $\alpha^m + \alpha^{-m} = 0$. D'où $\alpha^{2m} = -1$. Par conséquent $\alpha^{4m} = 1$. Ce qui signifie que $q \mid 4m$. D'où $m \geqslant \frac{q}{4}$. Ce qui termine la preuve. □

Lemme 2.29. *Soit p un nombre premier impair. Supposons que $h = h(p) < +\infty$. Nous avons :*

1. *$\alpha^k = 1$ si et seulement si $k \equiv 0 \pmod{4h}$.*
2. *$\alpha^k = -1$ si et seulement si $k \equiv 2h \pmod{4h}$.*

Démonstration.

1. Supposons que $\alpha^k = 1$. Alors, $q \mid k$. Comme par hypothèse p est un nombre premier impair et $h < +\infty$, alors d'après le théorème 2.28, $q = 4h$. Par conséquent $4h \mid k$. Ce qui signifie que $k \equiv 0 \pmod{4h}$.
   Réciproquement, supposons que $k \equiv 0 \pmod{4h}$, alors il existe $\ell \in \mathbb{Z}$ tel que $k = 4h\ell$. Par suite, $\alpha^k = (\alpha^{4h})^\ell$. Comme d'après le théorème 2.28, $q = 4h$, alors $\alpha^k = 1$.
2. Supposons que $\alpha^k = -1$. Selon le théorème 2.28, $q = 4h$, donc $\alpha^{2h} = -1$. Cela nous permet de déduire que, $\alpha^k = \alpha^{2h}$. Par suite $\alpha^{k-2h} = 1$. Donc $4h \mid k-2h$. Ce qui signifie que $k \equiv 2h \pmod{4h}$.
   Réciproquement, supposons que $k \equiv 2h \pmod{4h}$, alors $k = 4h\ell + 2h$, avec $\ell \in \mathbb{Z}$. Par suite, $\alpha^k = (\alpha^{4h})^\ell \alpha^{2h} = -1$.

□

La proposition suivante est d'une grande importance.

Proposition 2.30 ([1])**.** *Soit p un nombre premier. Supposons que $h = h(p) < +\infty$.*

1. *Si $p = 2$, alors $h = 1$ et pour tout entier $k \geqslant 0$,*

$$x_{2k} \equiv 1 \pmod 2 \quad \text{et} \quad x_{2k+1} \equiv 0 \pmod 2.$$

2. *Si p est impair alors*
   (a) *$x_k \equiv 1 \pmod p$ si et seulement si $k \equiv 0 \pmod{4h}$.*
   (b) *$x_k \equiv -1 \pmod p$ si et seulement si $k \equiv 2h \pmod{4h}$.*
   (c) *$x_k \equiv 0 \pmod p$ si et seulement si $k \equiv h \pmod{2h}$.*
   (d) *$4h \mid p-1$ ou $4h \mid p+1$.*

Démonstration.

1. Supposons que $p = 2$. D'après la relation (2.15),

$$u_k = \begin{cases} 1 & \text{si } k \text{ est pair} \\ u_1 & \text{si } k \text{ est impair} \end{cases}$$

Vu que par hypothèse $h(2)$ est fini, alors $u_1 = 0$. Comme pour tout entier $k \geqslant 0$, $u_k = \overline{x_k}$, alors $h(2) = 1$ et

— $x_k \equiv 1 \pmod 2$ si et seulement si $k \equiv 0 \pmod 2$

— $x_k \equiv 0 \pmod 2$ si et seulement si $k \equiv 1 \pmod 2$

Par conséquent, pour tout entier $k \geqslant 0$

$$x_{2k} \equiv 1 \pmod 2 \quad \text{et} \quad x_{2k+1} \equiv 0 \pmod 2.$$

2. Supposons que p est un nombre premier impair.

Vu que pour tout $k \geqslant 0$, $u_k = \overline{x_k}$, alors $x_k \equiv \pm 1 \pmod p$ si et seulement si $u_k = \pm 1$.

$$\begin{aligned} u_k = \pm 1 &\iff \frac{\alpha^k + \alpha^{-k}}{2} = \pm 1 \iff \alpha^{2k} + 1 = \pm 2\alpha^k \\ &\iff \left(\alpha^k\right)^2 \mp 2\alpha^k + 1 = 0 \\ &\iff \left(\alpha^k \mp 1\right)^2 = 0 \\ &\iff \alpha^k = \pm 1 \end{aligned}$$

Par conséquent

$$x_k \equiv \pm 1 \pmod p \text{ si et seulement si } \alpha^k = \pm 1.$$

La première et la seconde assertion du lemme 2.29 nous permettent de déduire que

(a) $x_k \equiv 1 \pmod p$ si et seulement si $k \equiv 0 \pmod{4h}$.

(b) $x_k \equiv -1 \pmod p$ si et seulement si $k \equiv 2h \pmod{4h}$.
Nous pouvons donc conclure que si $k \equiv 0 \pmod{2h}$, alors $x_k \equiv (-1)^{\frac{k}{2h}} \pmod p$.

(c) Pour tout entier $k \geqslant 0$, $x_k \equiv 0 \pmod p$ si et seulement si $u_k = 0$.

$$\begin{aligned} u_k = 0 &\iff \frac{\alpha^k + \alpha^{-k}}{2} = 0 \\ &\iff \alpha^{2k} + 1 = 0 \\ &\iff \alpha^{2k} = -1 \end{aligned}$$

Comme p est un nombre premier impair et $h < +\infty$, alors d'après le théorème 2.28, $\operatorname{ord}(\alpha) = 4h$. Par conséquent, $\alpha^{2h} = -1$. Nous avons alors, $u_k = 0$ si et seulement si $\alpha^{2k} = \alpha^{2h}$. Cela étant équivalent à $\operatorname{ord}(\alpha) \mid 2k - 2h$, nous obtenons alors l'équivalence suivante : $u_k = 0$ si et seulement si $4h \mid 2k - 2h$. Comme u_k est la classe d'équivalence de x_k. Alors $x_k \equiv 0 \pmod p$ si et seulement si $4h \mid 2k - 2h$. Ce qui est clairement équivalent à $k \equiv h \pmod{2h}$.
Conclusion : $x_k \equiv 0 \pmod p$ si et seulement si $k \equiv h \pmod{2h}$.

(d) Pour finir, prouvons la dernière assertion. Considérons le morphisme de corps $Frob : \overline{\mathbb{F}_p} \to \overline{\mathbb{F}_p}$ définie par $Frob(x) = x^p$. Comme $Frob$ est un morphisme de corps, alors

$$Frob(\alpha^2 - 2u_1\alpha + 1) = (\alpha^2)^p + (-2u_1)^p(\alpha)^p + 1.$$

Comme $-2u_1 \in \mathbb{F}_p$ et α est racine du polynôme $P(X) = X^2 - 2u_1X + 1 \in \mathbb{F}_p[X]$, alors

$$0 = Frob(\alpha^2 - 2u_1\alpha + 1) = (\alpha^p)^2 - 2u_1\alpha^p + 1.$$

Par conséquent, α^p est racine du polynôme P. Vu que le coefficient constant du polynôme P est égal à 1, alors ses racines sont α et α^{-1}. Il en résulte alors que $\alpha^p = \alpha$ ou $\alpha^p = \alpha^{-1}$. Par suite, $\alpha^{p-1} = 1$ ou $\alpha^{p+1} = 1$. Par conséquent, $\text{ord}(\alpha) \mid p-1$ ou $\text{ord}(\alpha) \mid p+1$. Comme p est un nombre premier impair et $h < +\infty$, alors d'après le théorème 2.28, $\text{ord}(\alpha) = 4h$. Ce qui termine la preuve.

□

Cette proposition permet de déduire facilement le lemme 2.27 dû à Lan et Szalay [11].

Démonstration du lemme 2.27. Soit $p \in \{2, 3, 5\}$. Supposons que $h(p) < +\infty$.

- Supposons que $p = 2$. D'après l'assertion 1 de la proposition 2.30, $h(2) = 1$.
- Supposons que $p = 3$. On a alors $x_1 \equiv 0, 1$ ou $-1 \pmod p$. Donc d'après la proposition 2.30, $h(3) \mid 1$. Par conséquent, $h(3) = 1$.
- Si $p = 5$, alors d'après la dernière assertion de la proposition 2.30, $4h(5) \mid 4$ ou $4h(5) \mid 6$. Comme $4 \nmid 6$, alors $4h(5) \mid 4$. Par conséquent, $h(5) = 1$.

□

Le corollaire suivant découle de la proposition 2.30. Nous l'appliquerons dans le prochain chapitre.

Corollaire 2.31 ([1])**.** *Soit p un nombre premier. S'il existe deux entiers positifs r et s, tels que $x_r \equiv \pm 1 \pmod p$, $x_s \equiv 0 \pmod p$ et $\text{pgcd}\,(y_r, y_s) = 1$, alors pour tout entier $k \geqslant 0$, $x_{2k+1} \equiv 0 \pmod p$ et $x_{2k} \equiv (-1)^k \pmod p$.*

Démonstration. Supposons qu'il existe deux entiers strictement positifs r et s tels que

$$x_r \equiv \pm 1 \pmod p \text{ et } x_s \equiv 0 \pmod p.$$

La seconde hypothèse nous garantit que $h = h\,(p) < +\infty$, donc d'après la proposition 2.30,

$$\begin{aligned} r &\equiv 0 \pmod{2h} \\ s &\equiv h \pmod{2h} \end{aligned}$$

Par suite, $h \mid r$ et $h \mid s$. Par conséquent, d'après la troisième assertion de la proposition 2.17, $y_h \mid y_r$ et $y_h \mid y_s$. Comme par hypothèse y_r et y_s sont premiers entre eux, alors $y_h = 1$. Rappelons que la suite $(y_k)_{k\geqslant 0}$ est une suite à coefficient dans $\mathbb{N}$, dont le premier terme y_0 est nul, et qui, selon le lemme 2.18 est strictement croissante. Donc $y_h = 1$ entraine nécessairement que $h = 1$. Pour compléter la preuve, il suffit d'appliquer la proposition 2.30 pour obtenir

$$x_{2k+1} \equiv 0 \pmod p \text{ et } x_{2k} \equiv (-1)^k \pmod p.$$

□

Nous arrivons à la fin de cette section, concluant avec le lemme suivant concernant la suite $(T_k(c))_{k\geqslant 0}$, où c est un entier strictement supérieur à 1. Ce dernier découle de la proposition 2.30. Il sera utilisé à plusieurs reprises dans le prochain chapitre.

Lemme 2.32 ([1])**.** *Soient p un nombre premier impair, $c > 1$ un entier et $h = h(p)$ l'indice de divisibilité de p dans $(T_k(c))_{k\geqslant 0}$. Supposons que $h < +\infty$. Nous avons :*

1. $T_k(c) \equiv 1 \pmod{p}$ *si et seulement si* $k \equiv 0 \pmod{4h}$.
2. $T_k(c) \equiv -1 \pmod{p}$ *si et seulement si* $k \equiv 2h \pmod{4h}$.
3. $T_k(c) \equiv 0 \pmod{p}$ *si et seulement si* $k \equiv h \pmod{2h}$.
4. *Si $p \mid c$ alors $h = 1$ et pour tout entier $k \geqslant 0$,*

$$T_{2k+1}(c) \equiv 0 \pmod{p} \text{ et } T_{2k}(c) \equiv (-1)^k \pmod{p}$$

Démonstration.

— Il est clair que $(c, 1)$ est la solution minimale de l'équation de Pell-Fermat

$$u^2 - (c^2 - 1)v^2 = 1.$$

Donc d'après le théorème 2.20, pour tout entier $k \geqslant 0$, $T_k(c) = x_k$. Alors en utilisant la proposition 2.30 nous obtenons les trois premières assertions.

— Supposons que $p \mid c$, comme $(c, 1)$ est la solution minimale de l'équation de Pell-Fermat

$$u^2 - (c^2 - 1)v^2 = 1,$$

alors $h = 1$. Par conséquent, en utilisant les trois premières assertions, nous obtenons $T_{2k+1}(c) \equiv 0 \pmod{p}$ et $T_{2k}(c) \equiv (-1)^k \pmod{p}$.

□

Chapitre 3

Sur l'équation diophantienne exponentielle $(a^n - 1)(b^m - 1) = x^2$

Szalay [18] est le premier à s'intéresser à l'étude de l'équation diophantienne

$$(a^n - 1)(b^n - 1) = x^2$$

d'inconnues $(n, x) \in \mathbb{N}^* \times \mathbb{N}^*$, où a et b sont deux entiers distincts et strictement supérieurs à 1. Cela en montrant que cette dernière n'admet pas de solutions lorsque $(a, b) = (2, 3)$. Par la suite, plusieurs auteurs ont obtenu de nouveaux résultats concernant cette équation, tels que Hajdu [7], Cohn [5], Le [11], Ishii [8], Noubissie, Togbé et Zhang [16]. Walsh [22], quant à lui, a été le premier à étudier l'équation diophantienne

$$(a^n - 1)(b^m - 1) = x^2,$$

d'inconnues n, m et x. Il a prouvé que cette équation n'a pas de solution en entiers strictement positifs n, m et x pour $(a, b) = (2, 3)$. Ensuite, Tang [19] a amélioré ce résultat en considérant le cas $a \equiv 2 \pmod 6$ et $b \equiv 3 \pmod{12}$.
Récemment, nous [1] avons généralisé quelques résultats des auteurs cités précédemment. Nous avons également étudié l'équation $(a^n - 1)(b^n - 1) = x^2$ dans le cas où $a^2 \equiv -1 \pmod p$, où $p \equiv 1 \pmod 8$ est un facteur premier de b. Ce chapitre, consacré à l'étude des équations diophantiennes exponentielles

$$(a^n - 1)(b^n - 1) = x^2 \text{ et } (a^n - 1)(b^m - 1) = x^2,$$

est composé de deux parties. Dans la première partie, nous rappellerons quelques propriétés du symbole de Legendre. Nous la clôturons par un lemme concernant le symbole de Legendre $\left(\frac{1\pm\iota}{p}\right)$, où $p = A^2 + B^2 \equiv 1 \pmod 4$ un nombre premier impair avec A impair, et ι est l'unique entier dans $\{0, 1, \ldots, p-1\}$ satisfaisant $\iota \equiv BA^{-1} \pmod p$. Dans la seconde partie, nous présenterons nos résultats.

3.1 Quelques propriétés du symbole de Legendre

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

$$a \equiv k^2 \pmod{b}.$$

Dans ce cas, on dit aussi que a est un carré modulo b.

Définition 3.1. *Soient p un nombre premier et a un entier. Le symbole de Legendre noté $\left(\frac{a}{p}\right)$ est l'entier défini comme suit :*

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

Le symbole de Legendre ne dépend que de la classe de a modulo p, autrement dit

$$a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Il vérifie le résultat suivant.

Théorème 3.2 (Critère d'Euler)**.** *Si p est un nombre premier impair, alors pour tout entier a :*

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

Démonstration. Si $a \equiv 0 \pmod{p}$ alors $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$. Par suite $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$. Supposons que a n'est pas divisible par p et posons β la classe de a modulo p. Alors $\beta \in (\mathbb{F}_p)^*$ qui, rappelons le, est un groupe cyclique d'ordre $p-1$. Soit η un générateur de $(\mathbb{F}_p)^*$. Il existe alors $k \in \mathbb{N}$ tel que $\beta = \eta^k$. Posons $\alpha = \beta^{\frac{p-1}{2}}$ alors $\alpha^2 = 1$. Autrement dit α est racine dans $\mathbb{F}_p$ du polynôme $X^2 - 1$, qui admet uniquement deux racines distinctes dans le corps $\mathbb{F}_p$, qui sont 1 et -1.

- Si $\alpha = 1$, alors $\beta^{\frac{p-1}{2}} = 1$. Par conséquent $\left(\eta^k\right)^{\frac{p-1}{2}} = 1$. Comme η est d'ordre $p-1$. Alors $\frac{k}{2}(p-1)$ est un multiple de $p-1$. Ce qui entraîne que $\frac{k}{2}$ est un entier. Ce qui signifie que $k = 2k'$ est un entier pair. Par conséquent $\beta = \left(\eta^{k'}\right)^2$. Donc $\left(\frac{a}{p}\right) = 1$.
- Si $\alpha = -1$, alors $\beta^{\frac{p-1}{2}} = -1$. Supposons par l'absurde que $\left(\frac{a}{p}\right) = 1$, alors β est un carré dans $(\mathbb{F}_p)^*$. Autrement dit il existe $\gamma \in (\mathbb{F}_p)^*$ tel que $\beta = \gamma^2$. Par conséquent $\beta^{\frac{p-1}{2}} = \gamma^{p-1}$. Or $(\mathbb{F}_p)^*$ est un groupe d'ordre $p-1$. Donc $\beta^{\frac{p-1}{2}} = \gamma^{p-1} = 1$. Ce qui contredit l'hypothèse $\beta^{\frac{p-1}{2}} = -1$. Conclusion $\left(\frac{a}{p}\right) = -1$.

□

En conséquence du critère d'Euler et du fait que pour tout nombre premier impair

$$(-1)^k \equiv (-1)^\ell \pmod{p} \Longrightarrow (-1)^k = (-1)^\ell,$$

nous obtenons les propriétés suivantes :

1. pour tout nombre premier impair p et pour tous $a, b \in \mathbb{Z}$,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

2. Pour tout nombre premier p impair

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{3.1}$$

Théorème 3.3. *Soit p un nombre premier impair, alors*

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

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

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

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

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

Calculons alors ϕ^p. Sachant que $\zeta^8 = 1$, $\zeta^4 = -1$ et $\phi^p = \zeta^p + \zeta^{-p}$ alors

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

Par conséquent,

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

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

Rappelons la loi de réciprocité quadratique.

Théorème 3.4 (La loi de réciprocité quadratique)**.** *Pour tous nombres premiers impairs p et q distincts, on a :*

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

Soit $p \equiv 1 \pmod 4$ un nombre premier. D'après le théorème des deux carrés de Fermat, il existe deux entiers positifs A et B avec A impair tels que $p = A^2 + B^2$. Il est clair que $A \in [\![1, p-1]\!]$. Par conséquent, A admet un inverse modulo p, que nous notons abusivement $\frac{1}{A}$. Soit ι l'unique entier dans $[\![0, p-1]\!]$ satisfaisant

$$\iota \equiv \frac{B}{A} \pmod p. \tag{3.2}$$

Donc,

$$\iota^2 \equiv \frac{p - A^2}{A^2} \equiv \frac{p}{A^2} - 1 \pmod p,$$

ce qui donne

$$\iota^2 \equiv -1 \pmod p. \tag{3.3}$$

La proposition suivante est dû à Dirichlet.

Proposition 3.5. *Soit $p = A^2 + B^2 \equiv 1 \pmod 4$ un nombre premier impair avec A impair, et soit ι l'entier défini par la relation* (3.2)*. Alors,*

$$2^{\frac{p-1}{4}} \equiv \iota^{\frac{AB}{2}} \pmod p.$$

Pour la démonstration nous nous sommes inspirés du livre [14] et nous aurons besoin des deux lemmes suivants.

Lemme 3.6. *Soit $p = A^2 + B^2 \equiv 1 \pmod 4$ un nombre premier impair avec A impair, alors*

$$\left(\frac{A}{p}\right) = 1.$$

Démonstration. Supposons que $A = \prod_{i=1}^{\ell} p_i$, où les p_i sont des nombres premiers impairs non nécessairement distincts. On a

$$\left(\frac{A}{p}\right) = \prod_{i=1}^{\ell} \left(\frac{p_i}{p}\right). \tag{3.4}$$

De la relation $p = A^2 + B^2$ on en déduit que pour tout $i \in [\![1, \ell]\!]$

$$p \equiv B^2 \pmod{p_i}.$$

Autrement dit $\left(\frac{p}{p_i}\right) = 1$. Par suite, grâce à la loi de réciprocité quadratique, donnée par le

théorème 3.4

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

Or $p \equiv 1 \pmod 4$. En d'autre termes, $\frac{p-1}{2}$ est pair. Donc $\left(\frac{p_i}{p}\right) = 1$. Compte tenu de ceci, la relation (3.4) donne $\left(\frac{A}{p}\right) = 1$. □

Lemme 3.7. *Soit $p = A^2 + B^2 \equiv 1 \pmod 4$ un nombre premier impair avec A impair, alors*

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

Démonstration. Posons $A + B = \prod_{i=1}^{m} q_i$, où les q_i sont des nombres premiers impairs qui ne sont pas forcément distincts. Puisque $p \equiv 1 \pmod 4$, alors grâce à la loi de réciprocité quadratique, donnée par le théorème 3.4, on a pour tout i

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

Par conséquent,

$$\left(\frac{A+B}{p}\right) = \prod_{i=1}^{m} \left(\frac{q_i}{p}\right) = \prod_{i=1}^{m} \left(\frac{p}{q_i}\right). \tag{3.5}$$

Des égalités $(A+B)^2 = p + 2AB$ et $A = (A+B) - B$ on déduit que pour tout $i \in [\![1, m]\!]$

$$p \equiv 2B^2 \pmod{q_i}.$$

Par suite, pour tout $i \in [\![1, m]\!]$

$$\left(\frac{p}{q_i}\right) = \left(\frac{2B^2}{q_i}\right) = \left(\frac{2}{q_i}\right)\left(\frac{B}{q_i}\right)^2.$$

Comme pour tout $i \in [\![1, m]\!]$, $q_i \nmid B$, alors

$$\left(\frac{p}{q_i}\right) = \left(\frac{2}{q_i}\right).$$

Le théorème 3.3 nous permet de déduire que

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

En tenant compte de cette égalité, la relation (3.5) donne :

$$\left(\frac{A+B}{p}\right) = \prod_{i=1}^{m} (-1)^{\frac{q_i^2-1}{8}} = (-1)^{\sum_{i=1}^{m} \frac{q_i^2-1}{8}}. \tag{3.6}$$

Pour tous entiers impairs λ, μ, on a

$$\begin{aligned}\left(\lambda^2-1\right) &\equiv 0 \pmod 8\\ \left(\mu^2-1\right) &\equiv 0 \pmod 8.\end{aligned}$$

Donc

$$\left(\lambda^2-1\right)\left(\mu^2-1\right) \equiv 0 \pmod{16}.$$

Par suite

$$\frac{\left(\lambda^2-1\right)\left(\mu^2-1\right)}{8} \equiv 0 \pmod 2.$$

Autrement dit

$$\frac{\lambda^2\mu^2-1}{8} \equiv \frac{\lambda^2-1}{8}+\frac{\mu^2-1}{8} \pmod 2.$$

On en déduit que

$$\sum_{i=1}^{m}\frac{q_i^2-1}{8} \equiv \frac{\left(\prod_{i=1}^{m} q_i^2\right)-1}{8} \equiv \frac{(A+B)^2-1}{8} \pmod 2.$$

Par conséquent, en utilisant la relation (3.6) nous obtenons :

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

□

Démonstration de la proposition 3.5 . Puisque $p \equiv 1 \pmod 4$ alors $\frac{p-1}{4}$ est un entier. Par suite

$$(A+B)^{\frac{p-1}{2}} = \left((A+B)^2\right)^{\frac{p-1}{4}} = \left(A^2+B^2+2AB\right)^{\frac{p-1}{4}}.$$

Comme par hypothèse $p = A^2+B^2$, alors d'après le théorème 3.2 (critère d'Euler),

$$\left(\frac{A+B}{p}\right) \equiv 2^{\frac{p-1}{4}}(AB)^{\frac{p-1}{4}} \pmod p.$$

Comme $\iota \equiv \frac{B}{A} \pmod p$, alors $B \equiv \iota A \pmod p$. Par suite,

$$\left(\frac{A+B}{p}\right) \equiv 2^{\frac{p-1}{4}}(A)^{\frac{p-1}{2}}\iota^{\frac{p-1}{4}} \pmod p.$$

D'après le lemme 3.6, $\left(\frac{A}{p}\right) = 1$, alors $A^{\frac{p-1}{2}} \equiv 1 \pmod p$. Par conséquent,

$$\left(\frac{A+B}{p}\right) \equiv 2^{\frac{p-1}{4}}\iota^{\frac{p-1}{4}} \pmod p. \tag{3.7}$$

En utilisant le lemme 3.7 et le fait que $p = A^2 + B^2$, nous obtenons :

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

De la congruence $\iota^2 \equiv -1 \pmod{p}$, on déduit que

$$\left(\frac{A+B}{p}\right) \equiv \iota^{\frac{p-1}{4}} \iota^{\frac{AB}{2}} \pmod{p}$$

En combinant cette relation avec la relation (3.7), on obtient $2^{\frac{p-1}{4}} \equiv \iota^{\frac{AB}{2}} \pmod{p}$. □

Nous allons maintenant établir un lemme concernant le symbole de Legendre $\left(\frac{1 \pm \iota}{p}\right)$, où ι est l'entier défini par la relation (3.2).

Lemme 3.8 ([1])**.** *Soit $p = A^2 + B^2$ un nombre premier impair avec A impair. Soit ι l'entier défini par* (3.2)*. Alors, $\left(\frac{1+\iota}{p}\right) = (-1)^{\frac{(A+B)^2-1}{8}}$ et $\left(\frac{1-\iota}{p}\right) = (-1)^{\frac{(A-B)^2-1}{8}}$.*

Démonstration. Posons $\epsilon = \pm 1$. D'après le théorème 3.2,

$$\left(\frac{1+\epsilon\iota}{p}\right) \equiv (1+\epsilon\iota)^{\frac{p-1}{2}} \pmod{p}.$$

Par suite,

$$\left(\frac{1+\epsilon\iota}{p}\right) \equiv ((1+\epsilon\iota)^2)^{\frac{p-1}{4}} \pmod{p}.$$

En utilisant la relation (3.3), nous obtenons :

$$\left(\frac{1+\epsilon\iota}{p}\right) \equiv 2^{\frac{p-1}{4}} (\epsilon\iota)^{\frac{p-1}{4}} \pmod{p}.$$

D'après la relation (3.3), ι est inversible modulo p, d'inverse $-\iota$ que nous notons ι^{-1}. Donc $\epsilon\iota = \iota^{\epsilon}$. En utilisant la congruence donnée par la proposition 3.5, nous obtenons :

$$\left(\frac{1+\epsilon\iota}{p}\right) \equiv \iota^{\frac{2AB+\epsilon(p-1)}{4}} \pmod{p}.$$

Comme par hypothèse $p = A^2 + B^2$, alors $2AB + \epsilon(p-1) = \epsilon((A+\epsilon B)^2 - 1)$. Et puisque A est impair et B est pair, alors $(A+\epsilon B)^2 - 1 \equiv 0 \pmod{8}$. Par suite,

$$\left(\frac{1+\epsilon\iota}{p}\right) \equiv (\iota^2)^{\frac{\epsilon((A+\epsilon B)^2-1)}{8}} \pmod{p}.$$

En utilisant à nouveau la relation (3.3), nous obtenons :

$$\left(\frac{1+\epsilon\iota}{p}\right) \equiv (-1^{\epsilon})^{\frac{(A+\epsilon B)^2-1}{8}} \equiv (-1)^{\frac{(A+\epsilon B)^2-1}{8}} \pmod{p}.$$

Comme $\left(\frac{1+\epsilon\iota}{p}\right) = \pm 1$, et p est un nombre premier impair, alors la congruence ci-dessus nous

permet de déduire que

$$\left(\frac{1+\epsilon\iota}{p}\right) = (-1)^{\frac{(A+\epsilon B)^2-1}{8}}.$$

□

3.2 Généralisation de certains résultats sur l'équation $(a^n-1)(b^m-1)=x^2$

En 2000, Walsh [22] a étudié l'équation diophantienne exponentielle

$$(a^n-1)(b^m-1)=x^2, \tag{3.8}$$

d'inconnues $(n,m,x)\in\mathbb{N}^*\times\mathbb{N}^*\times\mathbb{N}^*$, pour $(a,b)=(2,3)$. Il a montré que dans ce cas, cette dernière n'admet pas de solutions en entiers strictement positifs n, m et x. Onze ans plus tard, Tang [19] a repris cette équation, et il a pu amélioré le résultat obtenu par Walsh [22], ceci en prouvant que l'équation (3.8) n'a pas de solutions lorsque $a\equiv 2 \pmod 6$ et $b\equiv 3 \pmod{12}$. Le théorème suivant, que nous [1] avons récemment établi, généralise le résultat de Tang [19].

Théorème 3.9 ([1]). *Si $b\equiv -1 \pmod 4$ et b possède un facteur premier $p\equiv\pm 3 \pmod 8$ tel que $a\equiv p-1 \pmod{2p}$, alors l'équation (3.8) n'a pas de solutions en entiers strictement positif n, m et x.*

Pour la preuve nous avons besoin du lemme suivant :

Lemme 3.10 ([1]). *Si l'équation*

$$(a^n-1)(b^m-1)=x^2$$

admet une solution en entiers strictement positifs n, m et x, avec $n=2n'$ et $m=2m'$, alors il existe deux entiers strictement positifs r et s tels que $a^{n'}=x_r$, $b^{m'}=x_s$ et $\operatorname{pgcd}(y_r,y_s)=1$, où pour tout $k\geqslant 0$, (x_k,y_k) représente la k-ème solution d'une certaine équation de Pell-Fermat.

Démonstration. Supposons que l'équation (3.8) admet une solution en entiers strictement positifs n, m et x, avec $n=2n'$ et $m=2m'$. Posons $d=\operatorname{pgcd}\left(a^{2n'}-1,b^{2m'}-1\right)$, il existe alors k_1 et k_2 deux entiers positifs et premiers entre tels que

$$a^{2n'}-1=dk_1 \quad \text{et} \quad b^{2m'}-1=dk_2$$

Par conséquent,

$$d^2k_1k_2=x^2.$$

Comme k_1 et k_2 sont premiers entre eux, alors il existe deux entiers positifs y et z premiers entre eux tels que $k_1 = y^2$ et $k_2 = z^2$. Par suite,

$$(a^{n'})^2 - dy^2 = 1 \quad \text{et} \quad (b^{m'})^2 - dz^2 = 1.$$

Supposons qu'il existe un entier strictement positif d' tel que $d = (d')^2$. Par conséquent,

$$(a^{n'})^2 - dy^2 = \left(a^{n'} - d'y\right)\left(a^{n'} + d'y\right) = 1$$

Comme les entiers a, n', d' et y sont positifs, alors $a^{n'} + d'y = 1$. Mais comme $a > 1$, alors ceci est impossible. Donc d n'est pas un carré parfait. Par conséquent, $\left(a^{n'}, y\right)$ et $\left(b^{m'}, z\right)$ sont deux couples solutions de l'équation de Pell-Fermat $u^2 - dv^2 = 1$. Comme $a, b > 1$, alors il existe deux entiers strictement positifs r et s tels que $\left(a^{n'}, y\right) = (x_r, y_r)$ et $\left(b^{m'}, z\right) = (x_s, y_s)$. Comme y et z sont premiers entre eux, alors y_r et y_s le sont également. Ce qui termine la preuve. □

Démonstration du théorème 3.9. Supposons qu'il existe une solution en entiers strictement positifs (n, m, x) pour l'équation (3.8).

— Comme $a \equiv p - 1 \pmod{2p}$ et p est par hypothèse un nombre premier impair, alors a est pair. Par conséquent $a^n - 1 \equiv \pm 1 \pmod 4$. Et puisque $b \equiv -1 \pmod 4$, alors $b^m - 1 \equiv (-1)^m - 1 \pmod 4$. Par suite,

$$x^2 = (a^n - 1)(b^m - 1) \equiv \pm\left((-1)^m - 1\right) \pmod 4$$

En supposant que m est impair, nous obtenons $x^2 \equiv 2 \pmod 4$, ce qui est absurde. Donc m est pair. Il existe alors un entier strictement positif m' tel que $m = 2m'$.

— Vu que $a \equiv p - 1 \pmod{2p}$, alors $a \equiv -1 \pmod p$. Par conséquent, $a^n - 1 \equiv (-1)^n - 1 \pmod p$. Comme $b \equiv 0 \pmod p$, alors

$$x^2 = (a^n - 1)(b^m - 1) \equiv -\left((-1)^n - 1\right) \pmod p$$

En supposant que n est impair, nous obtenons $\left(\frac{2}{p}\right) = 1$. Donc, d'après le théorème 3.3, $p \equiv \pm 1 \pmod 8$. Ce qui contredit le fait que par hypothèse $p \equiv \pm 3 \pmod 8$. Nous déduisons que n est pair. D'où l'existence d'un certain entier strictement positif n' tel que $n = 2n'$.

Comme n et m sont pairs, alors il existe en vertu du lemme 3.10 deux entiers positifs r et s tels que

$$a^{n'} = x_r,\ b^{m'} = x_s \text{ et } \operatorname{pgcd}(y_r, y_s) = 1. \tag{3.9}$$

Comme $a \equiv -1 \pmod p$ et $b \equiv 0 \pmod p$, alors

$$x_r \equiv \pm 1 \pmod p \text{ et } x_s \equiv 0 \pmod p.$$

Par conséquent, l'indice r est d'après le corollaire 2.31 pair. D'où l'existence d'un certain entier positif r' tel que $r = 2r'$. Compte tenu de ce dernier fait et de la relation (3.9), nous obtenons :

$$a^{n'} = x_{2r'}.$$

Par conséquent, d'après la première assertion du corollaire 2.16, $a^{n'} = 2x_{r'}^2 - 1$. Donc $a^{n'}$ est impair. Or a est par hypothèse pair. D'où la contradiction. Nous concluons que l'équation (3.8) n'a pas de solutions en entiers strictement positifs n, m et x lorsque a et b satisfont les hypothèses du théorème. □

3.3 Quelques nouveaux résultats concernant l'équation $(a^n - 1)(b^n - 1) = x^2$

Dans cette section, nous allons étudier l'équation diophantienne $(a^n - 1)(b^n - 1) = x^2$ d'inconnues $(n, x) \in \mathbb{N}^* \times \mathbb{N}^*$, où a et b sont deux entiers distincts et strictement supérieurs à 1. Dans toute la suite, dans certains cas, on supposera que b est divisible par un nombre premier $p \equiv \pm 3 \pmod 8$, dans d'autres cas, on supposera qu'il est divisible par un nombre premier $p = A^2 + B^2 \equiv 1 \pmod 8$.

3.3.1 Cas où $a \equiv -1 \pmod p$

En 2016, en utilisant les solutions de l'équation de Pell-Fermat $u^2 - dv^2 = 1$, Ishii [8] a donné une condition nécessaire et suffisante pour l'existence de solutions pour l'équation

$$(a^n - 1)(b^n - 1) = x^2 \tag{3.10}$$

dans le cas où $a \equiv 5 \pmod 6$ et $b \equiv 0 \pmod 3$. Ci-dessous son résultat.

Théorème 3.11 ([8]). *Supposons que $a \equiv 5 \pmod 6$ et $b \equiv 0 \pmod 3$. Alors, l'équation (3.10) admet une solution en entiers strictement positifs (n, x) si et seulement si $(a, b) = (x_r, x_s)$ avec $d \equiv 2 \pmod 3$ un entier strictement positif, satisfaisant $x_1 \equiv 0 \pmod 3$, $r \equiv 2 \pmod 4$ et s impair. Dans ce cas la solution est $(n, x) = (2, dy_r y_s)$.*

Inspirés par ce résultat, Noubissie et Togbé [15] ont donné une condition nécessaire et suffisante pour l'existence de solutions pour l'équation (3.10) dans le cas où $a \equiv 4 \pmod 5$ et $b \equiv 0 \pmod 5$. Voici leur théorème.

Théorème 3.12 ([15]). *Supposons que $a \equiv 4 \pmod 5$ et $b \equiv 0 \pmod 5$. Alors, l'équation (3.10) admet une solution en entiers strictement positifs (n, x) si et seulement si $(a, b) = (x_r, x_s)$ avec $d \equiv \pm 1 \pmod 5$ un entier strictement positif et non carré, satisfaisant $x_1 \equiv 0 \pmod 5$, $r \equiv 2 \pmod 4$ et s impair. Dans ce cas la solution est $(n, x) = (2, dy_r y_s)$.*

En utilisant le lien entre les solutions à coordonnées positives de l'équation de Pell-Fermat et les polynômes de Tchebychev de première et de seconde espèce, nous [1] avons généralisé les théorèmes 3.11 et 3.12.

Théorème 3.13 ([1])**.** *Soit $p \equiv \pm 3 \pmod 8$ un nombre premier. L'équation* (3.10) *a une solution en entiers strictement positifs (n, x) avec $a \equiv -1 \pmod p$ et $b \equiv 0 \pmod p$ si et seulement s'il existe des entiers strictement positifs i, j et c tels que $a = T_{4i-2}(pc)$, $b = T_{2j-1}(pc)$. Dans ce cas $n = 2$ est l'unique solution.*

Démonstration. Supposons que $a \equiv -1 \pmod p$, $b \equiv 0 \pmod p$ et que l'équation (3.10) admet une solution en entiers strictement positifs (n, x). En utilisant les hypothèses faites sur a et b, nous obtenons les congruences suivantes :

$$a^n - 1 \equiv (-1)^n - 1 \pmod p \quad \text{et} \quad b^n - 1 \equiv -1 \pmod p.$$

Par suite,

$$x^2 \equiv -((-1)^n - 1) \pmod p.$$

Supposons que n est impair, alors $x^2 \equiv 2 \pmod p$. Par suite, $\left(\frac{2}{p}\right) = 1$. Donc, d'après le théorème 3.3, $p \equiv \pm 1 \pmod 8$. Ce qui contredit l'hypothèse $p \equiv \pm 3 \pmod 8$. Donc, ce que nous avons supposé est faux, n est pair. D'où l'existence d'un certain entier strictement positif n', tel que

$$n = 2n'. \tag{3.11}$$

Alors d'après le lemme 3.10, il existe deux entiers strictement positifs r et s tels que

$$a^{n'} = x_r,\ b^{n'} = x_s \text{ et } \operatorname{pgcd}(y_r, y_s) = 1, \tag{3.12}$$

où pour tout entier $k \geqslant 0$, (x_k, y_k) représente une solution à coordonnées positives d'une certaine équation de Pell-Fermat $u^2 - dv^2 = 1$. Comme $a \equiv -1 \pmod p$ et $b \equiv 0 \pmod p$, alors

$$x_r \equiv \pm 1 \pmod p \quad \text{et} \quad x_s \equiv 0 \pmod p.$$

Et comme $\operatorname{pgcd}(y_r, y_s) = 1$, alors il existe d'après le corollaire 2.31, des entiers strictement positifs c, i' et j tels que

$$x_1 = pc,\ r = 2i' \text{ et } s = 2j - 1. \tag{3.13}$$

D'après le théorème 2.20, $x_{2i'} = T_{2i'}(pc)$ et $x_{2j-1} = T_{2j-1}(pc)$. Donc en utilisant la relation (3.12), nous obtenons

$$a^{n'} = T_{2i'}(pc) \text{ et } b^{n'} = T_{2j-1}(pc). \tag{3.14}$$

D'après la dernière assertion du lemme 2.32, $T_{2i'}(pc) \equiv (-1)^{i'} \pmod p$. Comme

$$a \equiv -1 \pmod p,$$

alors $(-1)^{n'} \equiv (-1)^{i'} \pmod{p}$. En prouvant que $n' = 1$, nous pouvons aisément déduire l'existence d'un entier $i \in \mathbb{N}^*$ tel que $i' = 2i - 1$. Et dans ce cas la relation (3.14) entraîne

$$a = T_{4i-2}(pc) \text{ et } b = T_{2j}(pc).$$

Pour prouver que $n' = 1$, nous allons raisonner comme dans [8], [15] et [16].
Supposons que $n' \geqslant 3$. Comme d'après la relation (3.13), $r = 2i'$, alors en utilisant la relation (3.12) et la première assertion du corollaire 2.16, nous obtenons

$$a^{n'} = 2x_{i'}^2 - 1.$$

Par conséquent, $(x_{i'}, a, n')$ est solution de l'équation diophantienne $2x^2 - 1 = y^m$, d'inconnues x, y et m. D'après [3, Proposition 8.1] cette équation n'admet que $(1, 1, m)$ et $(78, 23, 3)$ comme solutions à coordonnées positives. A partir de cela et du fait que $a > 1$, nous déduisons que

$$(x_{i'}, a, n') = (78, 23, 3).$$

Comme $x_{i'} = 78$, et de la relation (3.13), s est impair, alors d'après la seconde assertion du lemme 2.19, $x_s \equiv 78 \pmod{156}$. Donc il existe $\ell \in \mathbb{Z}$ tel que $x_s = 156\ell + 78 = 2 \times 39 \times (2\ell + 1)$. Nous remarquons que $\nu_2(x_s) = 1$. Or, d'après la relation (3.12) et le fait que $n' = 3$, $x_s = b^3$. Donc $\nu_2(x_s) = 3\nu_2(b)$. Nous déduisons que ce que nous avons supposé est faux, $n' < 3$.
Supposons que $n' = 2$, alors d'après la relation (3.11), $n = 4$. Selon [5, Result 2] l'équation

$$(a^4 - 1)(b^4 - 1) = x^2$$

n'a de solutions que lorsque $\{a, b\} = \{13, 239\}$. Comme 13 et 239 sont des nombres premiers et par hypothèse $b \equiv 0 \pmod{p}$, alors $p = 13$ ou 239. Et aucun d'eux n'est congru à -1 modulo l'autre. Ce qui contredit l'hypothèse $a \equiv -1 \pmod{p}$. Ainsi l'hypothèse $n' = 2$ est fausse. Par conséquent $n' = 1$.
Réciproquement, supposons qu'il existe des entiers strictement positifs i, j et c tels que $a = T_{4i-2}(pc)$ et $b = T_{2j-1}(pc)$. D'après la dernière assertion du lemme 2.32,

$$a \equiv -1 \pmod{p} \text{ et } b \equiv 0 \pmod{p}.$$

Montrons maintenant que $n = 2$ est solution de l'équation (3.10). Comme $(pc, 1)$ est la solution minimale de l'équation de Pell-Fermat $u^2 - (p^2c^2 - 1)v^2 = 1$, alors d'après le théorème 2.20 pour tout entier $k \geqslant 1$,

$$T_k(pc) = x_k \text{ et } U_{k-1}(pc) = y_k.$$

D'où

$$\begin{aligned}(a^2-1)(b^2-1) &= ((T_{4i-2}(pc))^2-1)((T_{2j-1}(pc))^2-1)\\ &= ((p^2c^2-1)U_{4i-3}(pc)U_{2j-2}(pc))^2.\end{aligned}$$

□

Exemple 3.14. *Posons* $a = 18$ *et* $b = 19$. *On a* $a \equiv -1 \pmod{19}$ *et* $b \equiv 0 \pmod{19}$. *Comme*

$$(18^2-1)(19^2-1) = 17 \times 19 \times 18 \times 20 = 2^3 \times 3^2 \times 5 \times 17 \times 19,$$

alors d'après le théorème 3.13, l'équation $(18^n-1)(19^n-1) = x^2$ *n'a pas de solutions en entiers strictement positifs* n *et* x.

Exemple 3.15. *Posons* $a = 241$ *et* $b = 5291 = 11 \times 13 \times 37$. *On a*

$$a \equiv -1 \pmod{11} \qquad \text{et} \qquad 11 \equiv 3 \pmod{8},$$

et

$$(a^2-1)(b^2-1) = 240 \times 242 \times 5290 \times 5292 = \left(2^4 \times 3^2 \times 5 \times 7 \times 11 \times 23\right)^2.$$

Alors d'après le théorème 3.13, $(n, x) = (2, 2^4 \times 3^2 \times 5 \times 7 \times 11 \times 23)$ *est l'unique solution de l'équation* $(241^n-1)(5291^n-1) = x^2$.

3.3.2 Cas où $a \equiv tp-1 \pmod{2p^2}$ avec $t \in [\![1, 2p-1]\!]$

En 2010, Lan et Szalay [11] ont prouvé que l'équation (3.10) n'admet pas de solutions lorsque $a \equiv 2 \pmod 6$ et $b \equiv 0 \pmod 3$. En 2019, Noubissie et Togbé [15], quant à eux, ont traité l'équation (3.10) dans le cas où $a \equiv 4 \pmod{10}$ et $b \equiv 0 \pmod 5$, et ont prouvé que dans ce cas, l'équation (3.10) n'admet pas de solutions en entiers strictement positifs n et x. Le théorème suivant permet de généraliser ces deux résultats.

Théorème 3.16 ([1])**.** *S'il existe un facteur premier* p *de* b *et un entier* $t \in [\![1, 2p-1]\!]$ *tels que* $p \equiv \pm 3 \pmod 8$ *et* $a \equiv tp-1 \pmod{2p^2}$*, alors l'équation* (3.10) *n'a pas de solutions en entiers strictement positifs* n *et* x.

Démonstration. Supposons que l'équation (3.10) a une solution en entiers strictement positifs n et x. L'hypothèse $a \equiv tp-1 \pmod{2p^2}$ implique que $a \equiv -1 \pmod p$. Et comme par hypothèse $b \equiv 0 \pmod p$, alors d'après le théorème 3.13, il existe des entiers strictement positifs i, c tel que $a = T_{4i-2}(pc)$. Comme $(pc, 1)$ est la solution minimale de l'équation de Pell-Fermat $u^2-((pc)^2-1)v^2 = 1$, alors d'après le théorème 2.20, $a = x_{4i-2}$. Donc en utilisant la première assertion du corollaire 2.16, nous obtenons $a = 2x_{2i-1}^2-1$. En utilisant à nouveau le théorème 2.20, nous obtenons $a = 2T_{2i-1}^2(pc)-1$. Comme d'après lemme 2.32, $T_{2i-1}(pc) \equiv 0 \pmod p$, alors $a \equiv -1 \pmod{2p^2}$. En utilisant à nouveau l'hypothèse $a \equiv tp-1 \pmod{2p^2}$, nous obtenons $tp \equiv 0 \pmod{2p^2}$. Ce qui signifie que $2p \mid t$, ce qui contredit l'hypothèse

$t \leqslant 2p-1$. Conclusion : Avec les hypothèses posées sur a et b, l'équation (3.10) ne peut avoir de solutions en entiers strictement positifs n et x. □

Le théorème 3.16 donne, dans le cas particulier où $p \in \{3, 5\}$ les deux assertions suivantes, dues respectivement à Lan et Szalay [11] et à Noubissie et Togbé [15].

Corollaire 3.17. *Supposons que les conditions suivantes sont vérifiées*

1. $a \equiv 2 \pmod 6$ *et* $b \equiv 0 \pmod 3$,
2. $a \equiv 4 \pmod{10}$ *et* $b \equiv 0 \pmod 5$.

Alors l'équation (3.10) *n'a pas de solutions en entiers strictement positifs* n *et* x.

Démonstration.

1. Supposons que $a \equiv 2 \pmod 6$ et $b \equiv 0 \pmod 3$. Alors il existe un entier k tel que $a = 6k + 2$. Soit r le reste de la division euclidienne de k par 3, on a alors :

$$a = 6(3\ell + r) + 2, \text{ avec } \ell \in \mathbb{Z}.$$

   Donc $a \equiv 6r + 2 \pmod{18}$. En posant $t = 2r + 1$ et en tenant compte du fait que $0 \leqslant r \leqslant 2$, on obtient

$$a \equiv 3t - 1 \pmod{2 \times 3^2} \quad \text{et} \quad 1 \leqslant t \leqslant 5 = 2 \times 3 - 1.$$

   Comme $b \equiv 0 \pmod 3$, alors d'après le théorème 3.16, l'équation (3.10) n'a pas de solutions en entiers strictement positifs n et x.

2. Supposons maintenant que $a \equiv 4 \pmod{10}$ et $b \equiv 0 \pmod 5$. Donc $a = 10k + 4$, avec $k \in \mathbb{Z}$. Et comme il existe $(\ell, r) \in \mathbb{Z} \times [\![0, 4]\!]$ tel que $k = 5\ell + r$, alors $a = 50\ell + 10r + 4$. En posant $t = 2r + 1$, on obtient

$$a \equiv 5t - 1 \pmod{2 \times 5^2} \quad \text{et} \quad 1 \leqslant t \leqslant 2 \times 5 - 1.$$

   Puisque $b \equiv 0 \pmod 5$, selon le théorème 3.16, l'équation (3.10) n'a pas de solutions en entiers strictement positifs n et x.

□

3.3.3 Cas où $a \equiv 0 \pmod 2$ et $b \equiv -1 \pmod 4$

En 2011, Tang [19] a prouvé que l'équation (3.10) ne possède pas de solutions lorsque a pair et $b \equiv 15 \pmod{20}$. Noubissie, Togbé et Zhang [16] ont gardé l'hypothèse a pair et ont montré que si b est un nombre premier congru à 3 modulo 8, alors l'équation (3.10) ne possède pas de solutions. Quelques mois plus tard Noubissie et Togbé [15] ont amélioré leur résultat précédent en prouvant que l'équation (3.10) ne possède pas de solution lorsque $b \equiv 3 \pmod{12}$. Le théorème suivant permet de généraliser les trois résultats précédents.

Théorème 3.18 ([1]). *Si a est pair, $b \equiv -1 \pmod 4$ et b possède un facteur premier $p \equiv \pm 3 \pmod 8$, alors l'équation (3.10) n'a pas de solutions en entiers strictement positifs n et x.*

Démonstration. Procédons par l'absurde en supposant que l'équation (3.10) admet une solution en entiers strictement positifs n et x. Comme par hypothèse a est pair et $b \equiv -1 \pmod 4$, alors $a^n - 1 \equiv \pm 1 \pmod 4$ et $b^n - 1 \equiv (-1)^n - 1 \pmod 4$. Par suite,

$$x^2 \equiv \pm\left((-1)^n - 1\right) \pmod 4.$$

En Supposant que n est impair, nous obtenons : $x^2 \equiv 2 \pmod 4$. Or 2 n'est pas un carré modulo 4. Donc n est nécessairement pair, c'est-à-dire $n = 2n'$, où n' est un entier strictement positif. Puisque n est pair, alors il existe en vertu du lemme 3.10 deux entiers positifs r et s tels que

$$a^{n'} = x_r \text{ et } b^{n'} = x_s. \tag{3.15}$$

Comme a est pair, alors x_r l'est aussi. Par conséquent, $h(2)$ l'indice de divisibilité de 2 dans la suite $(x_k)_{k\geqslant 0}$ est fini. Dans ce cas, d'après l'assertion 1 de la proposition 2.30, pour tout entier $k \geqslant 0$, x_{2k} impair et x_{2k+1} pair. Donc, comme $x_s = b^{n'}$ et b est impair, alors s est pair. D'où l'existence d'un certain entier positif s' tel que $s = 2s'$. Par suite, en utilisant la relation (3.15) et la première assertion du corollaire 2.16, nous obtenons :

$$b^{n'} = 2x_{s'}^2 - 1.$$

Comme b possède un facteur premier $p \equiv \pm 3 \pmod 8$, alors

$$2x_{s'}^2 - 1 \equiv 0 \pmod p.$$

D'où

$$2x_{s'}^2 \equiv 1 \pmod p.$$

Par conséquent,

$$\left(\frac{2}{p}\right)\left(\frac{x_{s'}^2}{p}\right) = \left(\frac{2x_{s'}^2}{p}\right) = 1.$$

En d'autre termes $\left(\frac{2}{p}\right) = 1$. Ce qui contredit le fait que $p \equiv \pm 3 \pmod 8$. Nous concluons que ce que nous avons supposé tout au début de cette démonstration est faux, l'équation (3.10) n'a pas de solutions en entiers strictement positifs n et x pour a et b vérifiant les hypothèses du présent théorème. □

Dans le cas où $p \in \{3, 5\}$, le théorème 3.18 donne les trois assertions suivantes dues respectivement à Tang [19], Noubissie et al [16], et Noubissie et Togbé [15].

Corollaire 3.19. *Supposons que ces conditions sont vérifiées*

1. $a \equiv 0 \pmod 2$ *et* $b \equiv 15 \pmod{20}$.

2. $a \equiv 0 \pmod 2$*,* b *premier et* $b \equiv 3 \pmod 8$*.*

3. $a \equiv 0 \pmod 2$ *et* $b \equiv 3 \pmod{12}$*.*

Alors l'équation (3.10) *n'a pas de solutions en entiers strictement positifs* n *et* x*.*

Démonstration.

1. Comme $b \equiv 15 \pmod{20}$, alors $b \equiv 3 \pmod 4$ et $b \equiv 0 \pmod 5$. Vu que a est pair, alors d'après le théorème 3.18, l'équation (3.10) ne possède pas de solutions en entiers strictement positifs n et x.
2. Puisque $b \equiv 3 \pmod 8$, alors $b \equiv 3 \pmod 4$. Et comme b est un nombre premier et a est pair, alors a et b vérifient les hypothèses du théorème 3.18. Par conséquent, l'équation (3.10) n'admet pas de solutions en entiers strictement positifs n et x.
3. Étant donné que $b \equiv 3 \pmod{12}$, alors $b \equiv 3 \pmod 4$ et $b \equiv 0 \pmod 3$. Comme a est pair, alors selon le théorème 3.18, l'équation (3.10) n'a pas de solutions en entiers strictement positifs n et x.

□

3.3.4 Cas où $p = A^2 + B^2$ et $a^2 \equiv -1 \pmod p$

Il est important de noter que dans tous les résultats précédents, les hypothèses sur a et b ont été choisies d'une façon à ce que l'on puisse exclure le cas n impair. Dans les résultats à venir, toujours dans le but d'exclure le cas n impair, nous considérons le cas où $a^2 \equiv -1 \pmod p$. D'après (3.1), cette congruence est possible si et seulement si $p \equiv 1 \pmod 4$. Ce qui est, d'après le théorème des deux carrés de Fermat, équivalent à p est une somme de deux carrés. Commençons par le théorème suivant.

Théorème 3.20 ([1])**.** *Soit* $p = A^2 + B^2 = 1 \pmod 8$ *un facteur premier de* b *avec* $A + B \equiv \pm 3 \pmod 8$*. Si* $a^2 \equiv -1 \pmod p$*, alors l'équation* (3.10) *n'a pas de solutions en entiers strictement positifs* n, x *avec* n *impair.*

Démonstration. Supposons que A est impair, donc $A^2 \equiv 1 \pmod 8$. Comme par hypothèse $p = A^2 + B^2 = 1 \pmod 8$, alors $B^2 \equiv 0 \pmod 8$. Par conséquent, $B \equiv 0, 4 \pmod 8$. Par suite, $B \equiv -B \pmod 8$. D'où,

$$A + B \equiv A - B \pmod 8.$$

Puisque par hypothèse $A + B \equiv \pm 3 \pmod 8$, alors il en est de même pour $A - B$. Dans ce cas, $\dfrac{(A \pm B)^2 - 1}{8}$ est impair. Soit ι l'entier défini par (3.2). En appliquant le lemme 3.8, nous obtenons

$$\left(\frac{1+\iota}{p}\right) = \left(\frac{1-\iota}{p}\right) = -1. \tag{3.16}$$

De plus, comme $a^2 \equiv -1 \pmod p$, alors de (3.3), $a^2 \equiv \iota^2 \pmod p$. Par conséquent,

$$(a - \iota)(a + \iota) \equiv 0 \pmod p.$$

Par suite,

$$a \equiv \pm\iota \pmod{p}.$$

Supposons par l'absurde que l'équation (3.10) possède une solution en entiers strictement positif n et x avec n impair. Alors en utilisant la relation (3.3), nous obtenons

$$a^n - 1 \equiv \pm\iota - 1 \pmod{p}.$$

Vu que $b \equiv 0 \pmod{p}$, alors

$$x^2 = (a^n - 1)(b^n - 1) \equiv \pm\iota + 1 \pmod{p}.$$

D'où

$$\left(\frac{1+\iota}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{1-\iota}{p}\right) = 1.$$

Ce qui contredit (3.16). Par conséquent, n est pair. Nous pouvons donc déduire que ce que nous avons supposé est faux, l'équation (3.10) n'a pas de solutions avec n impair. □

Remarque 3.21. *Il est important de souligner que la condition* $A+B \equiv \pm 3 \pmod{8}$*, lorsque nous supposons* $p \equiv 1 \pmod{4}$*, n'est pas suffisante pour exclure le cas* n *impair, même si* $a^2 \equiv -1 \pmod{p}$ *et* $b \equiv 0 \pmod{p}$*. En effet, pour* $p = 5 = 1^2 + 2^2$*,* $a = (1+5k)^2 + 1$ *et* $b = (2+5\ell)^2 + 1$*, où* k *et* ℓ *sont des entiers quelconques,* $n = 1$ *est une solution de l'équation* $(a^n - 1)(b^n - 1) = x^2$*.*

Le théorème suivant découle de l'application du théorème 3.20 dans le cas où $p = 17$.

Théorème 3.22 ([1])**.** *L'équation* (3.10) *a une solution en entiers strictement positifs* (n, x) *sous les hypothèses* $a^2 \equiv -1 \pmod{17}$ *et* $b \equiv 0 \pmod{17}$ *si et seulement s'il existe des entiers positifs* r*,* s*,* c *et un entier impair* β *tels que* $a = T_r(c)$*,* $b = T_s(c)$ *avec* $c \equiv 9(3^\beta + 6^\beta) \pmod{17}$*,* $r \equiv \pm\beta \pmod{8}$ *et* $s \equiv 4 \pmod{8}$*. Dans ce cas,* $n = 2$ *est l'unique solution.*

Démonstration. Supposons que

$$a^2 \equiv -1 \pmod{17} \text{ et } b \equiv 0 \pmod{17}, \tag{3.17}$$

et que l'équation (3.10) possède une solution en entiers strictement positif n et x. Comme $p = 17 = 1^2 + 4^2$, alors d'après le théorème 3.20, n est pair. D'où l'existence d'un entier strictement positif n' tel que $n = 2n'$. Dans ce cas, le lemme 3.10 assure l'existence de deux entiers strictement positifs r et s tels que

$$a^{n\prime} = x_r \text{ et } b^{n\prime} = x_s. \tag{3.18}$$

Pour tout entier $k \geqslant 0$, posons $u_k = \overline{x_k}$, où $\overline{x_k}$ représente la classe d'équivalence de x_k modulo 17. D'après la relation (2.15), pour tout entier $k \geqslant 0$,

$$u_k = \frac{\alpha^k + \alpha^{-k}}{2}, \tag{3.19}$$

où α et α^{-1} sont les racines du polynôme $f(X) = X^2 - 2u_1X + 1$ dans une clôture algébrique de $\mathbb{F}_{17}$. Soit q l'ordre de α dans le groupe multiplicatif $\left(\overline{\mathbb{F}_{17}}\right)^*$. L'hypothèse $b \equiv 0 \pmod{17}$ et (3.18) impliquent que

$$x_s \equiv 0 \pmod{17}. \tag{3.20}$$

Donc $h(17)$ est fini. Dans ce cas, d'après le théorème 2.28, $q = 4h(17)$. Comme $p = 17$, alors d'après la dernière assertion de la proposition 2.30, $q \mid 16$. D'où, $\alpha^{16} = 1$. Par conséquent $\alpha \in (\mathbb{F}_{17})^*$. Vu que 3 est un générateur du groupe $(\mathbb{F}_{17})^*$, alors il existe $\beta \in [\![0, 15]\!]$, tel que

$$\alpha = 3^{\beta}. \tag{3.21}$$

Montrons que β est impair et que $r \equiv \pm\beta \pmod{8}$. Pour ce faire, commençons par montrer que n' est impair. Supposons par l'absurde que n' est pair. Selon [5, Result 2], l'équation (3.10) n'a de solutions que lorsque $n = 4$ avec$\{a, b\} = \{13, 239\}$. Or ceux-ci ne satisfont pas les conditions (3.17). On déduit alors que n' est impair. Par conséquent, en utilisant à nouveau la relation (3.17), nous obtenons : $a^{2n'} \equiv -1 \pmod{17}$. Donc, d'après la relation (3.18), $\overline{x_r}^2 \equiv -1 \pmod{17}$. D'où $u_r^2 = -1$. En utilisant la relation (3.19), nous obtenons ce qui suit :

$$\alpha^{2r} + \alpha^{-2r} + 2 = -4.$$

Par suite,

$$(\alpha^{2r})^2 + 6\alpha^{2r} + 1 = 0.$$

Par conséquent, α^{2r} est l'une des racines du polynôme $X^2 + 6X + 1 = (X - 2)(X - 9)$ dans $\mathbb{F}_{17}$. En d'autres termes $\alpha^{2r} \in \{3^2, 3^{-2}\}$. En utilisant la relation (3.21), nous obtenons : $3^{2r\beta} \in \{3^2, 3^{-2}\}$. Par suite, $3^{2r\beta-2} = 1$ ou $3^{2r\beta+2} = 1$. Comme $\mathrm{ord}(3) = 16$, alors

$$r\beta \equiv \pm 1 \pmod{8}.$$

Il en résulte de cette congruence que β est impair. Par suite, $\beta^2 \equiv 1 \pmod{8}$. Donc en multipliant la congruence ci-dessus par β, on obtient $r \equiv \pm\beta \pmod{8}$.
Montrons maintenant que $s \equiv 4 \pmod{8}$. Puisque β est impair, d'après la relation (3.21), α est un générateur du groupe multiplicatif $(\mathbb{F}_{17})^*$. Ce qui signifie que $q = \mathrm{ord}(\alpha) = 16$. Par conséquent, en vertu du lemme 2.28, nous avons $h(17) = 4$. Comme d'après (3.20),

$$x_s \equiv 0 \pmod{17},$$

alors en utilisant l'assertion (2c) de la proposition 2.30, on trouve que $s \equiv 4 \pmod{8}$.
Montrons que $n = 2$. Ce qui revient à prouver que $n' = 1$. Supposons que $n' \geqslant 3$. Comme s est pair, alors il existe s', tel que $s = 2s'$. En utilisant la relation (3.18) et la première assertion du corollaire 2.16, nous obtenons : $b^{n'} = 2x_{s'}^2 - 1$. Par conséquent, $(x_{s'}, b, n')$ est solution de l'équation diophantienne $2x^2 - 1 = y^m$, d'inconnues x, y et m. D'après [3, Proposition 8.1] cette équation n'admet que $(1, 1, m)$ et $(78, 23, 3)$ comme solutions à coordonnées positives.

A partir de cela et du fait que $b > 1$, nous déduisons que

$$(x_{s'}, b, n') = (78, 23, 3).$$

Ce qui contredit l'hypothèse $17 \mid b$. Donc $n' < 3$. Puisque nous avons déjà prouvé que n est impair, nécessairement $n' = 1$. Par conséquent, $n = 2$. Et à partir de la relation (3.18), $a = x_r$ et $b = x_s$. Par le théorème 2.20, nous obtenons $a = T_r(x_1)$ et $b = T_s(x_1)$. Donc il suffit de prendre $c = x_1$. D'après les relations (3.19) et (3.21), $u_1 = \dfrac{3^\beta + 3^{-\beta}}{2}$. Comme dans $\mathbb{F}_{17}$,

$$3^{-1} = 6 \quad \text{et} \quad 2^{-1} = 9,$$

alors $x_1 \equiv 9(3^\beta + 6^\beta) \pmod{17}$.
Réciproquement, supposons qu'il existe des entiers strictement positif r, s, c et un entier impair β tels que $a = T_r(c)$ et $b = T_s(c)$, avec $r \equiv \pm\beta \pmod 8$, $s \equiv 4 \pmod 8$ et

$$c = \frac{3^\beta + 3^{-\beta}}{2} \pmod{17}. \tag{3.22}$$

Comme $(c, 1)$ est la solution minimale de l'équation de Pell-Fermat $u^2 - (c^2 - 1)v^2 = 1$, alors d'après le théorème 2.20, pour tout entier $k \geqslant 0$,

$$T_k(c) = x_k \tag{3.23}$$

et pour tout entier $k \geqslant 1$,

$$U_{k-1}(c) = y_k.$$

Par conséquent,

$$(a^2 - 1)(b^2 - 1) = ((c^2 - 1)U_{r-1}(c)U_{s-1}(c))^2.$$

Ce qui signifie que $(2, (c^2 - 1)U_{r-1}(c)U_{s-1}(c))$ est un couple solution de l'équation (3.10).
Posons pour tout entier $k \geqslant 0$, $u_k = \overline{T_k(c)}$, où $\overline{T_k(c)}$ représente la classe d'équivalence de $T_k(c)$ modulo 17. La relation (3.23) nous permet de déduire que pour tout entier $k \geqslant 0$, $u_k = \overline{x_k}$. Alors, d'après l'exemple 2.23, la suite $(u_k)_{k\geqslant 0}$ est une suite récurrente linéaire, vérifiant pour tout $k \geqslant 0$, $u_{k+2} - 2cu_{k+1} + u_k = 0$. Posons

$$f(X) = X^2 - 2cX + 1 \in \mathbb{F}_{17}[X].$$

On déduit à partir de la congruence (3.22) que 3^β et $3^{-\beta}$ sont les racines du polynôme f dans $\mathbb{F}_{17}$. Posons $\alpha = 3^\beta$, alors d'après la relation (2.15)

$$u_k = \frac{\alpha^k + \alpha^{-k}}{2}. \tag{3.24}$$

Pour montrer que $a^2 \equiv -1 \pmod{17}$ et $17 \mid b$, il suffit de montrer que $u_s = 0$ et $u_r^2 = -1$.

Commençons par u_s. D'après la relation (3.24),

$$u_s = \alpha^{-s}\frac{\alpha^{2s}+1}{2}.$$

Comme par hypothèse $s \equiv 4 \pmod 8$, alors $2s \equiv 8 \pmod{16}$. Par suite, $\alpha^{2s} = \alpha^{16k+8}$. Comme β est impair et $\alpha = 3^\beta$, alors $ord(\alpha) = 16$. Par conséquent, $\alpha^{2s} = \alpha^8 = -1$. D'où, $u_s = 0$. Montrons maintenant que $u_r^2 = -1$. D'après la relation (3.24),

$$u_r^2 = \frac{\alpha^{2r}+\alpha^{-2r}+2}{4}.$$

Puisque $\alpha = 3^\beta$, alors

$$\alpha^{2r}+\alpha^{-2r} = 3^{2r\beta}+3^{-2r\beta}.$$

La congruence $r \equiv \pm\beta \pmod 8$ avec β impair donne $2r\beta \equiv \pm 2 \pmod{16}$. Comme 3 est un générateur de $\mathbb{F}_{17}^*$, alors

$$\alpha^{2r}+\alpha^{-2r} = 3^2+3^{-2} = 3^2+2.$$

Par conséquent, $u_r^2 = \frac{13}{4} = -1$. Ce qui termine la preuve. □

Nous sommes arrivés à la fin de ce chapitre, que nous clôturons avec ces deux exemples.

Exemple 3.23. *Posons $a = 106$ et $b = 102$. Il n'est pas difficile de vérifier que $a^2 \equiv -1 \pmod{17}$ et $b \equiv 0 \pmod{17}$. Comme $(106^2-1)(102^2-1) = 3\times 5\times 7\times 101\times 103\times 107$ n'est pas un carré, alors d'après le théorème 3.22, l'équation $(106^n-1)(102^n-1) = x^2$ n'a pas de solutions en entiers strictement positifs n et x.*

Exemple 3.24. *Posons $a = 4$ et $b = 1921 = 17\times 113$. On a*

$$a^2 \equiv -1 \pmod{17}, \quad b \equiv 0 \pmod{17}$$

et

$$(a^2-1)(b^2-1) = 3\times 5\times 1920\times 1922 = \left(2^4\times 3\times 5\times 31\right)^2.$$

Donc d'après le théorème 3.22, $(n,x) = (2, 2^4\times 3\times 5\times 31)$ est l'unique solution de l'équation

$$\left(4^n-1\right)\left(1921^n-1\right) = x^2.$$

Conclusion et perspectives

Cette thèse a été consacrée à l'étude des équations diophantiennes exponentielles de la forme $(a^n-1)(b^n-1)=x^2$ et $(a^n-1)(b^m-1)=x^2$, d'inconnues $(n,m,x)\in\mathbb{N}^*\times\mathbb{N}^*\times\mathbb{N}^*$, où a et b sont deux entiers distincts et strictement supérieurs à 1.

Dans le premier chapitre, nous nous sommes intéressés à la théorie des fractions continues. Nous avons rappelé quelques définitions et donner des preuves détaillées de quelques résultats classiques de cette théorie. Nous avons également étudié le développement en fraction continue d'un nombre irrationnel quadratique, qui est un outil essentiel à la résolution de l'équation de Pell-Fermat.

Dans le deuxième chapitre, après avoir démontré que l'équation de Pell-Fermat admet une infinité de solutions, donner le lien entre ses solutions à coordonnées positives et les polynômes de Tchebychev de première et seconde espèces. Nous avons établit de nouveaux résultats concernant des congruences vérifiées par les solutions de l'équation de Pell-Fermat.

Dans le troisième et dernier chapitre, nous avons rappelé quelques propriétés du symbole de Legendre, et nous avons présenté de nouveaux résultats concernant les équations diophantiennes $(a^n-1)(b^n-1)=x^2$ et $(a^n-1)(b^m-1)=x^2$.

Nous terminons par quelques perspectives. D'après le théorème 3.16, si l'équation

$$(a^n-1)(b^n-1)=x^2$$

admet une solution (n,x) en entiers strictement positifs avec $a\equiv -1 \pmod p$, où $p\equiv \pm 3 \pmod 8$ est un facteur premier de b, alors

$$(n,x)=(2,dy_ry_s),$$

où $d=\operatorname{pgcd}(a^2-1,b^2-1)$ et (x_r,y_r) et (x_s,y_s) sont deux couples solutions de l'équation de pell-Fermat

$$u^2-dv^2=1.$$

Il est intéressant de voir si sous les conditions faites sur a et b, dy_ry_s est un carré, ou bien de chercher ce qu'il faudrait rajouter comme hypothèses au théorème 3.16, pour que cela soit satisfait. Il est également intéressant d'étudier par exemple l'équation $(a^n-1)(b^m-1)=x^r$, avec r impair.

Bibliographie

[1] Z. Ameur, R. Boumahdi, and T. Garici, *Some results concerning the exponential diophantine equation* $(a^n - 1)(b^m - 1) = x^2$, Indian Journal of Pure and Applied Mathematics, (2023), pp. 1–10.

[2] A. Baker, *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

[3] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Can. J. Math., 56 (2004), pp. 23–54.

[4] B. Buraux-Bourgeois, *Diophantine analysis in Lagrange*, in Analyse diophantienne et géométrie algébrique. Exposés du Séminaire d'Histoire des Mathématiques de l'Institut Henri Poincaré, Paris : Université Pierre et Marie Curie, Lab. de Mathématiques Fondamentales, 1993, pp. 13–23.

[5] J. H. E. Cohn, *The Diophantine equation* $(a^n - 1)(b^n - 1) = x^2$, Period. Math. Hung., 44 (2002), pp. 169–175.

[6] É. Galois, *Analyse algébrique. démonstration d'un théorème sur les fractions continues périodiques*, in Annales de mathématiques pures et appliquées, vol. 19, 1828, pp. 294–301.

[7] L. Hajdu and L. Szalay, *On the Diophantine equations* $(2^n - 1)(6^n - 1) = x^2$ *and* $(a^n - 1)(a^{kn} - 1) = x^2$, Period. Math. Hung., 40 (2000), pp. 141–145.

[8] K. Ishii, *On the expontential Diophantine equation* $(a^n - 1)(b^n - 1) = x^2$, Publ. Math. Debrecen, 89 (2016), pp. 253–256.

[9] T. Koshy, *Elementary number theory with applications*, Academic press, 2002.

[10] ——, *Pell and Pell-Lucas numbers with applications*, vol. 431, Springer, 2014.

[11] L. Lan and L. Szalay, *On the exponential diophantine equation* $(a^n - 1)(b^n - 1) = x^2$, Publ. Math. Debrecen, 77 (2010), pp. 465–470.

[12] M. Le, *A note on the exponential Diophantine equation* $(2^n - 1)(b^n - 1) = x^2$, Publ. Math. Debrecen, 74 (2009), pp. 401–403.

[13] A.-M. Legendre, *Essai sur la théorie des nombres*, Paris : Duprat ; Paris : Crapelet, 1798.

[14] F. Lemmermeyer, *Reciprocity laws. From Euler to Eisenstein*, Berlin : Springer, 2000.

[15] A. Noubissie and A. Togbé, *A note on the exponential Diophantine equation* $(a^n - 1)(b^n - 1) = x^2$, Ann. Math. Inform., 50 (2019), pp. 159–165.

[16] A. Noubissie, A. Togbé, and Z. Zhang, *On the exponential Diophantine equation* $(a^n - 1)(b^n - 1) = x^2$, Bull. Belg. Math. Soc. - Simon Stevin, 27 (2020), pp. 161–166.

[17] A. M. Rockett et al., *Continued fractions*, World Scientific, 1992.

[18] L. Szalay, *On the diophantine equation* $(2^n - 1)(3^n - 1) = x^2$, Publ. Math. Debrecen, 57 (2000), pp. 1–9.

[19] M. Tang, *A note on the exponential Diophantine equation* $(a^m - 1)(b^n - 1) = x^2$, J. Math. Res. Expo., 31 (2011), pp. 1064–1066.

[20] J. Trignan, *Introduction aux problèmes d'approximation : fractions continues, différences finies*, Éditions du Choix, 1994.

[21] R. W. Van der Waall, *On the Diophantine equations* $x^2 + x + 1 = 3v^2, x^3 - 1 = 2y^2, x^3 + 1 = 2y^2$, Simon Stevin, 46 (1972), pp. 39–51.

[22] P. G. Walsh, *On Diophantine equations of the form* $(x^n - 1)(y^m - 1) = z^2$, Tatra Mt. Math. Publ., 20 (2000), pp. 87–89.

Faculté de Mathématiques, USTHB
12 juillet 2024