N° d'ordre : 04/2018–D/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIENE

FACULTÉ DE MATHÉMATIQUES

THÈSE

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

En : MATHÉMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : **Rachid BOUMAHDI**

Sujet :

Contribution à l'étude de congruences de familles de nombres remarquables et équations diophantiennes

Soutenue publiquement, le **19/04/2018**, devant le jury composé de :

M.	BENSEBA B.	Maître de conférences /A à l'USTHB	Président
M.	BENCHERIF F.	Professeur à l'USTHB	Directeur de thèse
M.	KIHEL O.	Professeur à Brock University - Canada	Co-directeur de thèse
M.	AIBOUDI M.	Maître de conférences /A à l'U.A.B.O. Es sania	Examinateur
M.	AYAD M.	Maître de conférences /HDR à ULCO -France	Examinateur
M.	CHERCHEM A.	Maître de conférences /A à l'USTHB	Examinateur

Remerciements

J'aimerai exprimer ici toute ma reconnaissance aux membres du Jury qui ont accepté d'examiner ma thèse ainsi qu'à tous ceux qui ont contribué à l'aboutissement de ce travail.

Je remercie tout d'abord mes deux directeurs de thèse, le Professeur Farid Bencherif de la Faculté de Mathématiques de l'USTHB et le Professeur Omar Kihel du département de Mathématiques de Brock University (Canada) pour tout le temps qu'ils m'ont consacré pour m'initier à deux thèmes passionnants essentiels et complémentaires de la Théorie des Nombres qui font l'objet de cette thèse : la Théorie des congruences et la Théorie des équations diophantiennes.

J'ai eu le plaisir de retrouver comme directeur de ma thèse de doctorat mon Professeur d'Algèbre de mes années de graduation, le Professeur Farid Bencherif. Cela m'a permis d'apprécier de nouveau sa rigueur, sa disponibilité et sa compétence durant ces années de thèse. Il m'a initié à l'étude captivante des congruences de nombres et de polynômes remarquables portant des noms prestigieux : Bernoulli, Euler, Bell, Stirling, Fibonacci, Lucas, Morley, Wolstenholme, Babbage, Carlitz,...

Il m'a prodigué de précieux conseils pour la rédaction de ma thèse. Ses paroles d'encouragement ainsi que celles de son épouse m'ont beaucoup ému et ont grandement contribué à l'aboutissement de ce travail.

Le Professeur Omar Kihel m'a accueilli chaleureusement durant de nombreux mois au département de mathématiques de Brock University. Il m'a fait découvrir les techniques subtiles et surprenantes de résolution de certaines équations diophantiennes, les approximations diophantiennes, l'étude des formes quadratiques et l'étude des polynômes à valeurs entières. Grâce à lui, j'ai pu aussi participer à deux conférences internationales importantes, l'une à Bangkok en 2016, l'autre à Ostrava, en République Tchèque en 2017. Ces deux conférences m'ont permis d'avoir l'opportunité de pouvoir discuter avec d'autres éminents mathématiciens spécialistes de la théorie des nombres.

Je garde ainsi un merveilleux souvenir de mon séjour à Brock University à St. Catharines au Canada, de mes discussions, presque quotidiennes, à Starbucks avec le Professeur Omar Kihel, des diners au fameux restaurant "Le Mandarin" et de nos promenades près des Chutes du Niagara.

Je remercie chaleureusement le Professeur Boualem Benseba , Directeur du laboratoire LA3C pour l'honneur qu'il me fait en ayant accepter de présider ce Jury. Il a le souci permanent de vouloir faire progresser la recherche au sein du laboratoire qu'il dirige avec beaucoup de compétence et de rigueur. Merci Boualem.

J'exprime au Professeur Mohammed Aïboudi de la Faculté des Sciences Exactes et Appliquées de l'Université d'Oran 1 Ahmed Ben Bella, Vice Doyen de la Post Graduation, de la Recherche Scientifique et des Relations Extérieures mes vifs remerciements pour avoir accepter avec enthousiasme d'examiner cette thèse.

Je suis très sensible à l'honneur que me fait le Professeur Mohamed Ayad de l'Université du Littoral-Côte-d'Opale en ayant accepté de faire partie de ce Jury. J'ai beaucoup apprécié ses livres sur la Théorie de Galois qui m'ont été d'un grand apport, ainsi que les conférences enrichissantes qu'il a données au Canada et en Algérie, et que j'ai suivies avec beaucoup d'intérêt ces dernières années.

J'exprime ma profonde gratitude au Professeur Ahmed Cherchem de la Faculté de Mathématiques de l'USTHB pour avoir accepté d'examiner ce travail et pour toutes les discussions fructueuses que nous avons pu avoir ensemble.

Enfin, je ne saurais oublier de remercier tout particulièrement toutes les personnes qui ont contribué à l'aboutissement de ce travail. Mon ami Tarek Garici, l'icône de la Faculté de Mathématiques de l'USTHB. Il m'a apporté une aide considérable : rigueur mathématique, critiques constructives, conseils pour le Tex et Latex, soutien logistique (Café, Coca), conseils administratifs... en un mot je lui dis : Bravo Tarek ! Je remercie également le Professeur Abdelmoumène Zékiri pour les nombreuses et précieuses corrections de mes essais et pour son sens inégalable de l'humour ! Il est responsable du Séminaire d'Arithmétique. Il contribue à assurer efficacement une bonne ambiance de travail au sein du laboratoire LA3C.

Je remercie le Professeur Abdelhafid Berrachedi de la Faculté de Mathématiques pour sa sagesse, sa présence positive et imperturbable et ses judicieux conseils. Ainsi que le Professeur Sadek Bouroubi pour son soutien, et ses encouragements.

Le Professeur Abdelkader Necer de l'Université de Limoges m'a accueilli, en septembre 2014, au sein du prestigieux laboratoire XLIM de l'Université de Limoges. Il m'a beaucoup encouragé. Je suis heureux de lui dire que la conférence que j'ai donnée au Séminaire de ce Laboratoire a fait l'objet d'un article publié dernièrement.

Je remercie mes chers amis de parcours, Samir et Hamma, que j'ai connus au début des années 90, quand nous étions étudiants à l'USTHB, pour leurs encouragements sans relâche et leur aide sans faille depuis notre rencontre.

Je souhaite aussi exprimer ma profonde gratitude à Messieurs Bousse Allouche et Attou Seghier. Tous deux m'ont apporté un immense réconfort et une aide inestimable pendant mon séjour à St. Catharines. Le Docteur Bousse Allouche, un homme d'une riche culture, auteur d'une étude critique sur Albert Camus m'a aussi littéralement envoûté par ses discussions philosophiques et culturelles.

Table des matières

Notations

1. $\mathbb{N} = \{0, 1, 2, \ldots\}$: ensemble des entiers naturels.
2. $\mathbb{N}^* = \{1, 2, \ldots\}$: ensemble des entiers naturels non nuls.
3. $\mathbb{Z}$: l'ensemble des entiers rationnels.
4. $\mathbb{Q}$: l'ensemble des nombres rationnels.
5. $\mathbb{R}$: l'ensemble des nombres réels.
6. $\mathbb{C}$: l'ensemble des nombres complexes.
7. $\mathcal{P}$: l'ensemble des nombres premiers.
8. $\mathbb{F}_p$: le corps fini à p éléments.
9. $\deg P(x)$: le degré du polynôme $P(x)$.
10. $\text{pgcd}(a, b)$: le plus grand commun diviseur de a et b.
11. $\mathbb{Z}_{(p)}$: Anneau des $p-$entiers.
12. $\binom{n}{p}$: coefficient binomial.
13. H_m : le m-ième nombre harmonique généralisé.
14. $v_p(n)$: la valuation p-adique de l'entier n. C'est la plus grande puissance de p qui divise n.
15. $\text{num}(x)$: numérateur d'un rationnel.
16. $\text{denum}(x)$: dénominateur d'un rationnel.
17. $K[x]$: Polynômes à coefficients dans K.
18. $H(P)$: la hauteur d'un polynôme.
19. Δ : le premier opérateur de différence finie.
20. B_n : le n-ième nombre de Bernoulli.
21. F_n : le n-ième nombre de Fibonacci.
22. L_n : le n-ième nombre de Lucas.
23. $\lfloor x \rfloor$: la partie entière d'un nombre réel x, i.e. l'unique entier rationnel k vérifiant : $x - 1 < k \leqslant x$.
24. $a \equiv k \pmod{n}$ a est congru à k modulo p.
25. $\left(\frac{n}{p}\right)$: le symbole de Legendre.

Introduction

" Wir müssen wissen, wir werden wissen". (Nous devons savoir, nous saurons)
David Hilbert

Cette thèse est consacrée à l'analyse de certaines congruences de familles de nombres remarquables, ainsi qu'à l'étude de certaines équations diophantiennes quadratiques et de polynômes à coefficients entiers dont les valeurs sont des puissances d'entiers. Ce travail comporte trois parties.

Dans le premier chapitre, on donne des rappels concernant les congruences. Après avoir rappelé les principales propriétés des congruences, les théorèmes de Wilson, de Fermat, et d'Euler, la loi de réciprocité quadratique, nous précisons et étudions la notion de congruence dans l'anneau $\mathbb{Z}_{(p)}$ des p-entiers, p étant un nombre premier ; un p-entier est un nombre rationnel de valuation p-adique positive ou nulle. L'étude des congruences, modulo une puissance de p, des coefficients binomiaux centraux $\binom{2n}{n}$ pour $n = p$ et pour $n = \frac{p-1}{2}$, où $p \geqslant 3$, est un nombre premier, a une longue histoire. Celle-ci a débuté avec une congruence modulo p^2, pour $\binom{2p}{p} = 2\binom{2p-1}{p-1}$, découverte par Babbage en 1819 et qui se poursuit jusqu'à nos jours. Il s'agit de résulats obtenus par Wolstenholme en 1862, Morley en 1895, Glaisher en 1900, Carlitz en 1953, McIntosh en 1995, Zhao en 2007, Tauraso en 2010, Meštrović en 2014 et Rosen en 2013. Ce chapitre est ensuite dédié à une étude de congruences de familles de nombres remarquables tels que les nombres de Fibonacci, les nombres de Lucas, les nombres de Pell, les nombres de Pell-Lucas. Nous exposerons dans ce chapitre un résulat qui est une généralisation à la fois des congruences de Wolstenholme et de Morley et qui généralise aussi les différentes améliorations de ces congruences obtenues par d'autres auteurs. Plus précisément, nous généralisons les congruences suivantes de Wolstenholme et de Morley :

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3},$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^3},$$

en établissant la congruence modulo p^7 suivante pour le coefficient binomial $\binom{\alpha p-1}{p-1}$ où α est un p-entier [4]. Pour tout nombre premier impair $p \neq 7$ et pour tout p-entier α, on a

$$\binom{\alpha p-1}{p-1} \equiv 1 - \alpha(\alpha-1)(\alpha^2-\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k} + \alpha^2(\alpha-1)^2p^2\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij} \pmod{p^7}.$$

Le deuxième chapitre s'intitule " Etude de certaines équations diophantiennes quadratiques". Dans de nombreux cas, on utilise l'outil des congruences pour les résoudre. Nous commençons par des rappels historiques avant de passer à une étude détaillée des équations de Pell. Ceci nous amènera à étudier le développement en fraction continue d'un réel quadratique. On expliquera comment les fractions continues permettent de fournir un moyen rapide et relativement efficace pour le calcul de la solution fondamentale de l'équation de Pell $x^2 - dy^2 = 1$. On étudiera aussi l'équation générale de Pell $x^2 - dy^2 = C$ pour C dans $\mathbb{Z}$. Il s'agit, ici, de résoudre des équations diophantiennes de la forme

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

où a, b, c, d, e et f sont des entiers fixés. Lorsque l'on étudie une équation diophantienne donnée, la principale question qu'on se pose est de savoir s'il existe au moins une solution et dans le cas affirmatif, de déterminer le nombre de solutions et leur forme générale.

En 2012, dans [22], Keskin, Karaatli et Siar ont étudié l'équation diophantienne

$$x^2 - kxy + y^2 + 2^n = 0, \tag{1}$$

pour $0 \leqslant n \leqslant 10$ et $k \in \mathbb{N}^*$. Ils ont déterminé, pour ces différentes valeurs de n, les valeurs de k pour lesquelles l'équation (1) admet une infinité de solutions (x, y). Ils ont de plus, donné explicitement les solutions à l'aide des nombres de Fibonacci généralisés.

En 2013, dans [23], Keskin, Siar et Karaatli ont étudié l'équation diophantienne

$$x^2 - kxy + y^2 - 2^n = 0, \tag{2}$$

pour $0 \leqslant n \leqslant 10$ et $k \in \mathbb{N}^*$. Ils ont déterminé pour ces différentes valeurs de n, les valeurs de k pour lesquelles l'équation (2) admet une infinité de solutions (x, y). Ils ont aussi déterminé explicitement ces solutions à l'aide des nombres de Fibonacci généralisés. Cette étude les a amené à formuler la conjecture suivante :

Conjecture *Soit l'équation diophantienne*

$$x^2 - kxy + y^2 = 2^n \tag{3}$$

1. *Pour n impair et $n \geqslant 3$, on a :*
   - *Si $k > 2^n - 2$, l'équation (3) n'admet pas de solution entière positive.*
   - *Si $k \leqslant 2^n - 2$ et l'équation (3) admet une solution, alors k est pair.*
2. *Pour n pair et $n \geqslant 2$, on a :*
   - *Si $k > 2^n - 2$, l'équation (3) n'admet pas de solution entière impaire,*
   - *Si $k \leqslant 2^n - 2$ et l'équation (3) admet une solution positive impaire, alors k pair.*

En 2016, nous avons apporté une réponse positive à cette conjecture, nous avons aussi établi un résulat analogue pour l'équation diophantienne $x^2+y^2+kxy = -2^n$ qui est énoncé dans le théorème suivant :

Théorème 1. *[6] Soit l'équation diophantienne*

$$x^2 - kxy + y^2 = -2^n. \tag{4}$$

1. *Pour n impair et $n \geqslant 3$, on a :*
   - *Si $k > 2^n + 2$, l'équation (4) n'admet pas de solution entière positive.*
   - *Si $k \leqslant 2^n + 2$, et l'équation (4) admet des solution, alors k est pair.*
2. *Pour n pair et $n \geqslant 2$, on a :*
   - *Si $k > 2^n + 2$, l'équation (4) n'admet pas de solution positive impaire.*
   - *Si $k \leqslant 2^n + 2$, et l'équation (4) admet une solution positive impaire, alors k est pair et non divisible par 4.*

Dans ce chapitre deux, nous analysons minutieusement les travaux de Keskin, Siar et Karaatli dans ([22] et [23]). Nous le clôturons par un exposé de la preuve de la conjecture ci-dessus suivie de démonstrastion du théorème précédent.

Le chapitre trois est dédié aux Polynômes à coefficients entiers dont les valeurs des entiers sont des puissances d'entiers. Shapiro [46] a montré que, si les valeurs de P un polynôme à coefficients entiers, de degré n, sur un nombre infini de blocs d'entiers consécutifs sont de la forme $Q(m)$, où Q est un polynôme à coefficients entiers, alors $P(x) = Q(R(x))$ pour un certain polynôme R. Nous montrerons que, si les valeurs de P en un nombre fini de blocs d'entiers consécutifs, chacun plus

grand qu'une certaine borne, sont de la forme m^q où q est un diviseur de n, alors $P(x) = (R(x))^q$ pour un certain polynôme $R(x)$.

Enfin, nous concluons cette thèse par un énoncé des différentes perspectives de recherche que cette étude nous a permis d'envisager.

Chapitre 1

Congruences de familles de nombres remarquables

"*Le problème où l'on se propose de distinguer les nombres premiers des nombres composés...est connu comme l'un des plus importants et des plus utiles de toute l'Arithmétique...En outre, la dignité de la science semble demander que l'on recherche avec soin tous les secours nécessaires pour parvenir à la solution d'un problème si élégant et si célèbre.*"

Johann Carl Friedrich Gauss ([11] art. 329)

1.1 Introduction

La notion de congruence est trés ancienne. Bien qu'elle trouve son origine dans un passé lointain, il aura fallu attendre le XVIII-ième siècle, notamment avec Gauss, pour que la théorie des congruences soit formulée et developpée dans un langage mathématique rigoureux. Avant Gauss, la notion de congruence avait déjà été utilisée par Euler, Lagrange et Legendre. On doit à Gauss le formalisme et les notations des congruences que l'on utilise encore de nos jours.

1.2 Congruences dans l'anneau $\mathbb{Z}$

Dans son célèbre et immortel ouvrage intitulé Recherches arithmétiques [11], C. F. Gauss commence par mettre en place les notations et les propriétés des congruences dans l'anneau $\mathbb{Z}$ avant d'étudier la représentation d'un entier par une forme quadratique. Cet ouvrage d'un peu plus de 500 pages qui fut publié pour la première fois en 1801 alors que Gauss né en 1777 n'avait que 24 ans, fait encore référence de nos jours. Les définitions et les notations qu'il donne sont exactement celles qu'on utilise encore de nos jours. La toute première page de cet ouvrage débute comme suit :

"*Si un nombre a divise la différence des nombres b et c, b et c sont dits congrus suivant a, sinon incongrus. a s'appellera le module* ; *chacun des nombres b et c, résidus de l'autre dans le premier cas, et non résidus dans le second.*

Les nombres peuvent être positifs ou négatifs, mais entiers. Quant au module il doit évidemment être pris absolument, c'est à dire sans aucun signe."

Quelques lignes plus loin, en page 2 de [11] Gauss écrit : ,

"*Nous désignerons dorénavant la congruence de deux nombres par ce signe $\equiv$, en y joignant, lorsqu'il sera nécéssaire, le module renforcé entre parenthèses, ainsi* $-16 \equiv 9 \pmod 5$, $-7 \equiv 15 \pmod{11}$"

Comme on peut le constater, le vocabulaire et les notations de Gauss sont toujours d'actualité. Pour le moderniser quelque peu, nous pouvons affirmer, conformément à ce qu'affirma Gauss, qu' étant donné un entier naturel n et $(a, b) \in \mathbb{Z}^2$, on convient de dire que a est congru à b modulo n et

d'écrire $a \equiv b \pmod{n}$ si $a-b \in n\mathbb{Z}$. Cette relation appelée relation de congruence modulo n est une relation d'équivalence dans l'ensemble $\mathbb{Z}$ compatible avec l'addition et la multiplication de l'anneau $\mathbb{Z}$. Plus généralement, étant donné un anneau commutatif unitaire A, on convient aussi d'appeler "congruence dans l'anneau A toute relation d'équivalence $\mathcal{R}$ définie sur l'anneau A compatible avec l'addition et la mutiplication de cet anneau. Il est alors facile de constater que pour toute congruence définie sur l'anneau A, la classe de O_A (élément neutre du groupe additif $(A,+)$) est un idéal $\mathcal{I}$ de l'anneau A. Dire que deux éléments a et b sont congrus modulo $\mathcal{R}$ équivaut alors à dire que $a-b \in \mathcal{I}$. L'ensemble quotient $A/\mathcal{R}$ n'est rien d'autre que l'anneau quotient $A/\mathcal{I}$. De plus à tout idéal de l'anneau A correspond, par ce procédé, une congruence sur l'anneau A. Ainsi, dans le cas particulier de l'anneau $\mathbb{Z}$, les idéaux de $\mathbb{Z}$ étant les $n\mathbb{Z}$ où $n \in \mathbb{N}$, on retouve bien notre définition de congruence modulo n. On supposera que $n \geqslant 2$ car le cas où $n = 0$ correspond à l'égalité et le cas où $n = 1$ correspond au cas où tout entier est congru à tout autre entier.

Nous allons maintenant donner l'énoncé de théorèmes classiques, mais importants, concernant les congruences dans l'anneau $\mathbb{Z}$. Nous commencerons par le théorème connu aujourd'hui sous le nom de théorème de Wilson mais dont on reconnait que l'énoncé était déjà connu du célèbre mathématicien, philosophe, physiologiste et physicien Ibn al-Haytham (Bassora, 965-Le Caire, 1039). Selon Roshdi Rashed [41], cet énoncé devrait s'appeler Théorème d'Al-Haytham-Leibniz-Wilson-Waring-Lagrange-Euler-Gauss. Voici l'énoncé de ce théorème.

Théorème 1.1. *([16]) Un entier p strictement plus grand que 1 est un nombre premier si et seulement si $(p-1)! + 1 \equiv 0 \pmod{p}$.*

Le théorème de Wilson fournit une caractérisation des nombres premiers. C'est donc clairement un critère de primalité. Malheureusement son coût d'un point de vue algorithmique le rend inutilisable pour tester la primalité de grands nombres. Signalons que l'étude de la caractérisation des nombres premiers est un sujet d'actualité [1].

Le théorème suivant est connu sous le nom de "Petit théorème de Fermat".

Théorème 1.2. ***(Petit théorème de Fermat)*** *([16]) Si p est un nombre premier et si a est un entier non divisible par p, alors $a^{p-1} - 1 \equiv 0 \pmod{p}$.*

La preuve de ce théorème est immédiate. Si p est un nombre premier, on sait que l'anneau $\mathbb{Z}/p\mathbb{Z}$ est alors un corps. Si a est un entier non divisible par p, l'élément $\overline{a} = a + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^*$. Le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ étant d'ordre $p-1$, on a $\overline{a}^{p-1} = \overline{1}$, ce qui équivaut à affirmer que l'on a $a^{p-1} - 1 \equiv 0 \pmod{p}$.

Signalons que le petit théorème de Fermat a d'intéressantes conséquences. On en déduit de manière évidente un critère de non-primalité. Euler a généralisé le petit théorème de Fermat. En introduisant la fonction indicatrice d'Euler φ définie comme suit

$$\begin{array}{rl} \varphi : \mathbb{N}^* & \longrightarrow \mathbb{N}^* \\ n & \longmapsto \varphi(n) = \operatorname{card}\left\{x \in \mathbb{N}^* \ / \ x \leqslant n \text{ et } \ x \text{ est premier avec } n\right\}, \end{array}$$

le théorème d'Euler s'énonce comme suit :

Théorème 1.3 (Théorème d'Euler [16])**.** *Pour tout entier $n > 0$ et tout entier a premier avec n, on a $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

La démonstration du théorème d'Euler est immédiate. Soit n un entier naturel non nul. Si $n = 1$, on a nécessairement $a = 1$ et la congruence est bien vérifiée. Si $n \geqslant 2$, on constate avec le théorème de Bézout, que le groupe des unités de l'anneau $\mathbb{Z}/n\mathbb{Z}$ est

$$U\left(\mathbb{Z}/n\mathbb{Z}\right) = \left\{\overline{k} \ / \ 1 \leqslant k \leqslant n \text{ et } \ k \text{ est premier avec } n\right\}.$$

On a donc

$$\operatorname{card} U\left(\mathbb{Z}/n\mathbb{Z}\right) = \varphi(n)$$

Pour tout entier a premier avec n, on a : $\overline{a} = a + n\mathbb{Z} \in U\left(\mathbb{Z}/n\mathbb{Z}\right)$. Le groupe multiplicatif $U\left(\mathbb{Z}/n\mathbb{Z}\right)$ étant d'ordre $\varphi(n)$ on a $\overline{a}^{\varphi(n)} = \overline{1}$, ce qui équivaut à affirmer que l'on a $a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$.

Pour p premier, on a pour $n = p$, $\varphi(n) = \varphi(p) = p - 1$. L'application du théorème d'Euler pour $n = p$ fournit le théorème de Fermat. Le petit théorème de Fermat (ou le théorème d'Euler) a de nombreuses applications. L'une d'entre elles est le critère suivant connu sous le nom de critère d'Euler : il permet de caractériser les carrés modulo p.

Théorème 1.4 (**Critère d'Euler**). *Pour tout nombre premier impair p et tout entier a, on a*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 0 \pmod{p} \text{ si } p \mid a, \\ 1 \pmod{p} \text{ si } p \nmid a \text{ et s'il existe } x \in \mathbb{Z} \text{ tel que } x^2 \equiv a \pmod{p}, \\ -1 \pmod{p} \text{ si } p \nmid a \text{ et si pour tout } x \in \mathbb{Z}, \text{ on a } x^2 \not\equiv a \pmod{p}. \end{cases}$$

La définition suivante va nous permettre de reformuler le critère d'Euler d'une manière plus intéressante, en vue de ses applications.

Définition 1.5. *Soit p un nombre premier impair et a un entier tels que* $\operatorname{pgcd}(a, p) = 1$. *On considère la congruence*

$$x \in \mathbb{Z} \text{ et } x^2 \equiv a \pmod{p}. \tag{1.1}$$

1. *Si la congruence (1.1) possède (au moins) une solution, on dit que a est résidu quadratique modulo p.*
2. *Si la congruence (1.1) n'a pas de solution, on dit que a n'est pas résidu quadratique modulo p.*

Rappelons alors la définition du symbole de Legendre.

Définition 1.6. *Soit p un nombre premier impair et soit $a \in \mathbb{Z}$, on définit le symbole de Legendre $\left(\frac{a}{p}\right)$ comme suit*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p \mid a, \\ +1 \text{ si } p \nmid a \text{ et si } a \text{ est congru à un carré modulo } p, \\ -1 \text{ si } p \nmid a \text{ et si } a \text{ n'est pas congru un carré modulo } p. \end{cases}$$

On montre facilement, grâce au critère d'Euler la multiplicativité suivante du symbole de Legendre. Pour tous entiers a et b et pour tout nombre premier p, on a :

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

On peut alors reformuler le critère d'Euler comme suit :

Théorème 1.7 (Critère d'Euler). *Soit p un nombre premier impair. Alors, pour tout nombre entier a, on a*

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

Le théorème suivant est l'un des plus célèbres en Théorie des nombres.

Théorème 1.8. *Si p et q sont deux nombres premiers impairs, alors les congruences*

$$x^2 \equiv p \pmod{q} \quad \text{et} \quad x^2 \equiv q \pmod{p}$$

ont des solutions sauf dans le cas où p et q sont tous deux congrus à 3 modulo 4 auquel cas seule l'une de ces deux congruences possède des solutions.

Avec le symbole de Legendre, ce théorème peut se reformuler ainsi

Théorème 1.9 (**Loi de réciprocité quadratique**). *Si p et q sont deux nombres premiers impairs, on a*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Gauss appelait ce théorème le "aureum theorema" (théorème d'Or). Il le considérait comme l'un des joyaux de l'Arithmétique. L'histoire de ce théorème est fabuleuse. Euler chercha pendant 40 ans, en vain une preuve, il conjectura le résultat en 1783. Legendre reformula ce résultat en founissant une preuve qui, malheureusement, s'avéra incomplète. En 1796, Gauss (alors agé seulement de 19 ans) fut finalement le premier à publier une première preuve correcte de ce théorème. Gauss donna , au total, huit démonstrations de la loi de réciprocité quadratique dans ses "Disquisitiones arithmeticae" [11] publié en 1801. On dénombre aujourd'hui plus d'une centaine de preuves de ce théorème.

Théorème 1.10 (**Lois complémentaires**). *Pour tout nombre premier $p > 2$, on a*

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

1.2.1 Applications aux nombres de Fibonacci

La suite $(F_n)_{n\geqslant 0}$ des nombres de Fibonacci et la suite des nombres de Lucas $(L_n)_{n\geqslant 0}$ sont définies par les relations suivantes

$$\begin{aligned} F_0 &= 0,\ F_1 = 1 \text{ et } F_n = F_{n-1} + F_{n-2} \text{ pour } n \geqslant 2, \\ L_0 &= 2,\ L_1 = 1 \text{ et } L_n = L_{n-1} + L_{n-2} \text{ pour } n \geqslant 2. \end{aligned}$$

Les premiers termes de ces suites sont

$$\begin{aligned} (F_n)_{n\geqslant 0} &= (0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233 \ldots), \\ (L_n)_{n\geqslant 0} &= (2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521 \ldots). \end{aligned}$$

Les nombres de Fibonacci jouent un rôle important dans de nombreuses branches des mathématiques (voir [14], pp. 290-291).

Les suites de Fibonacci et de Lucas sont respectivement répertoriées $A000045$ et $A000032$ dans l'encyclopédie des suites d'entiers Sloane [47].

Les congruences suivantes sont bien connues, pour p premier on a

$$F_p \equiv \left(\frac{p}{5}\right) \pmod{p} \quad \text{et} \quad F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p}$$

Comme les solutions des équations diophantiennes étudiées par Keskin, Siar et Karaatli (section 2.4.2.) s'expriment à l'aide des nombres de Fibonacci généralisés et des nombres de Lucas généralisés, nous rappelons que

La suite de Fibonacci généralisée $(F_n(k,s))_{n\in\mathbb{N}}$ est définie pour $(k,s) \in \mathbb{Z}\times\mathbb{Z}^*$ par :

$$F_0(k,s) = 0, F_1(k,s) = 1 \text{ et } F_{n+1}(k,s) = kF_n(k,s) + sF_{n-1}(k,s), n \geqslant 1,$$

la suite de Fibonacci généralisée pour les indices négatifs par

$$F_{-n}(k,s) = \frac{-F_n(k,s)}{(-s)^n}, n \geqslant 1$$

pour $k = s = 1$ on retrouve la suite de Fibonacci classique définie ci-dessus. Pour $k = 2$ et $s = 1$ la suite $(F_n(2,1))_{n\in\mathbb{N}}$ est dite de Pell et elle est notée P_n.

La suite de Lucas généralisée $(L_n(k,s))_{n\in\mathbb{N}}$ est définie pour $(k,s) \in \mathbb{Z}\times\mathbb{Z}^*$ comme suit :

$$L_0(k,s) = 2, L_1(k,s) = k \text{ et } L_{n+1}(k,s) = kL_n(k,s) + sL_{n-1}(k,s), n \geqslant 1,$$

la suite de Lucas généralisée pour les indices négatifs par

$$L_{-n}(k,s) = \frac{-L_n(k,s)}{(-s)^n}, n \geqslant 1$$

pour $k = s = 1$ on retrouve la suite classique de Lucas définie ci-dessus. Pour $k = 2$ et $s = 1$. la suite $(L_n(2,1))_{n\in\mathbb{N}}$ est dite de Pell-Lucas et elle est notée L_n.

Terminons par les propriétés classiques des suites de Fibonacci généralisées.

Proposition 1.11. *([14]) Si $k^2 + 4s > 0$ et α , β sont les deux racines du trinôme $x^2 - kx - s$, alors*

$$F_n(k,-1) = -F_{-n}(k,-1).$$
$$F_n(k,s) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \text{ (Binet).}$$
$$F_n^2(k,-1) - kF_n(k,-1)F_{n-1}(k,-1) + F^2(k,-1) = 1.$$

1.3 Congruences dans un groupe et congruences dans l'anneau $\mathbb{Z}_{(n)}$

1.3.1 Congruences dans un groupe

Soit G un groupe additif commutatif. On définit une congruence dans le groupe G comme étant une relation d'équivalence compatible avec l'addition du groupe. Il est facile de prouver que, si H étant un sous-groupe de G, la relation $\mathcal{R}$ définie sur G par

$$x\mathcal{R}y \Longleftrightarrow x - y \in H$$

définit une congruence dans le groupe G. De plus, toute congruence $\mathcal{R}$ définie dans G est de cette forme, le groupe H étant constitué des éléments de la classe de l'élément neutre de G.

Cette notion est couramment employée. Ainsi $2\pi\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$ et on exprime pour $x, y \in \mathbb{R}$, l'égalité entre $\cos x$ et $\cos y$ en écrivant que l'on a $x \equiv \pm y \pmod{2\pi}$, c'est à dire que $x \pm y \in 2\pi\mathbb{Z}$.

Une autre congruence utile dans le groupe additif $\mathbb{Q}$ est la congruence modulo 1 qui est obtenue en considérant le sous-groupe $\mathbb{Z}$ de $\mathbb{Q}$. Cette congruence est définie comme suit pour x, $y \in \mathbb{Q}$: $x \equiv y \pmod 1 \Longleftrightarrow x - y \in \mathbb{Z}$. Cette congruence concerne la suite des nombres de Bernoulli qui est la suite de nombres rationnels $(B_n)_{n\in\mathbb{N}}$ qui a pour série génératrice exponentielle :

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

Ces nombres sont aussi définis plus simplement par les relations :

$$B_0 = 1 \text{ et } B_n = -\frac{1}{n+1}\sum_{k=0}^{n-1}\binom{n+1}{k}B_k,\ n \geqslant 1$$

Le théorème suivant, dit de Von Staudt-Clausen fut découvert en 1840 par deux mathématiciens indépendamment l'un de l'autre : Von Staudt (1798-1867) mathématicien allemand qui fut élève de Gauss et Clausen (1801-1885) mathématicien danois autodidacte.

Théorème 1.12 (**Théorème de von Staudt-Clausen**). *Pour tout entier naturel n pair ainsi que pour $n = 1$, on a*

$$-B_n \equiv \sum_{\substack{p \text{ premier} \\ et\ (p-1)|2n}} \frac{1}{p} \pmod 1$$

Ce théorème ne fait qu'exprimer le fait que

$$B_{2n} + \sum_{\substack{p \text{ premier} \\ et\ (p-1)|2n}} \frac{1}{p} \in \mathbb{Z}.$$

Une autre congruence célèbre est la congruence de Kummer dans le groupe additif $\mathbb{Q}$ des nombres rationnels.

Théorème 1.13. *Soit p un nombre premier impair, a et b deux entiers naturels non nuls tels que $p - 1 \nmid a$ et $a \equiv b \pmod{(p-1)}$, alors on a*

$$\frac{B_a}{a} \equiv \frac{B_b}{b} \pmod p.$$

Ce théorème ne fait qu'exprimer le fait que

$$\frac{B_a}{a} - \frac{B_b}{b} \in p\mathbb{Z}.$$

1.3.2 Congruences dans l'anneau $\mathbb{Z}_{(p)}$

Désignons par $\mathcal{P}$ l'ensemble des nombres premiers. Soit x un nombre rationnel non nul. Alors il existe une unique famille d'entiers $(v_p(x))_{p\in\mathcal{P}}$ ne comportant qu'un nombre fini d'éléments non nuls telle que

$$x = \varepsilon \prod_{p\,\in\mathcal{P}} p^{v_p(x)} \text{ avec } \varepsilon \in \{-1, 1\}$$

$v_p(x)$ est la valuation p-adique de x. Si $x = 0$, on pose $v_p(0) = \infty$. On pose aussi pour $x \neq 0$:

$$\text{num}(x) = \epsilon \prod_{p\,\in\mathcal{P} \text{ et } v_p(x)\geqslant 0} p^{v_p(x)} \quad \text{et} \quad \text{denum}(x) = \prod_{p\,\in\mathcal{P} \text{ et } v_p(x)\leqslant 0} p^{v_p(x)}.$$

Soit n une entier naturel non nul. On désigne par $\mathbb{Z}_{(n)}$ l'ensemble suivant :

$$\mathbb{Z}_{(n)} = \{x \in \mathbb{Q} \,/\, \text{pgcd}(\text{num}(x), n) = 1\}.$$

On montre facilement que $\mathbb{Z}_{(n)}$ est un sous-anneau de $\mathbb{Q}$ contenant $\mathbb{Z}$.

$$\mathbb{Z} \subset \mathbb{Z}_{(n)} \subset \mathbb{Q}.$$

Par ailleurs, on montre que pour x, $y \in \mathbb{Q}$, $p \in \mathcal{P}$

$$v_p(x+y) \geqslant \min(v_p(x), v_p(x))$$

et pour tous $x_k \in \mathbb{Q}$, $k = 1, ..., n$

$$v_p\left(\sum_{k=1}^{n} x_k\right) \geqslant \min(v_p(x_k))_{1 \leqslant k \leqslant n}$$

Pour $x = 0$, on pose $\text{num}(0) = 0$ et $\text{denum}(0) = 1$. On définit

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \ / \ v_p(x) \geqslant 0\},$$

on a alors aussi :

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \ / \ p \nmid \text{denum}(x)\}.$$

$\mathbb{Z}_{(p)}$ est un sous-anneau de $\mathbb{Q}$. Les éléments de $\mathbb{Z}_{(p)}$ sont appelés des p-entiers.

Pour $m \in \mathbb{N}^*$, on a

$$\mathbb{Z}_{(p^m)} = \mathbb{Z}_{(p)}.$$

La congruence modulo p^m dans $\mathbb{Z}$ définie par

$$\forall x, y \in \mathbb{Z},\ x \equiv y \pmod{p^m} \Longleftrightarrow x - y \in p^m\mathbb{Z},$$

peut alors s'écrire :

$$\forall x, y \in \mathbb{Z},\ x \equiv y \pmod{p^m} \Longleftrightarrow v_p(x-y) \geqslant m.$$

On constate ainsi que la congruence modulo p^m dans $\mathbb{Z}$ se prolonge en une congruence modulo p^m dans l'anneau $\mathbb{Z}_{(p)}$, c'est-à-dire en relation d'équivalence compatible avec l'addition et la multiplication définies sur $\mathbb{Z}_{(p)}$, en posant :

$$\forall x, y \in \mathbb{Z}_{(p)},\ x \equiv y \pmod{p^m} \Longleftrightarrow v_p(x-y) \geqslant m.$$

On a, en effet :

$$\forall x, y \in \mathbb{Z}, x \equiv y \pmod{p^m} \Longleftrightarrow x - y \in p^m\mathbb{Z}_{(p)}.$$

1.3.3 Propriétés de l'anneau $\mathbb{Z}_{(p)}$

On montre facilement que l'anneau $\mathbb{Z}_{(p)}$ est un anneau principal et que tout idéal de $\mathbb{Z}_{(p)}$ est de la forme $p^m\mathbb{Z}_{(p)}$. Le groupe des unités de l'anneau $\mathbb{Z}_{(p)}$ est

$$U\left(\mathbb{Z}_{(p)}\right) = \{x \in \mathbb{Q} \ / \ v_p(x) = 0\}.$$

1.4 Congruences pour des coefficients binomiaux

Dans tout ce qui suit, p désigne un nombre premier $p > 2$. On a déja vu que le fameux théorème de Wilson est un critère de primalité. De nombreux mathématiciens ont cherché d'autres critères de primalité. Ainsi dès 1819, Babbage [2] énonce le critère de primalité suivant :

$$\forall n \geqslant 2, \quad n \in \mathcal{P} \iff \forall m \in \{0, 1, 2, \ldots, n-1\}, \binom{n+m}{n} \equiv 1 \pmod{n}.$$

Signalons qu'en 2013, Meštrović [35] a généralisé ce critère en prouvant que pour tout $n, k \geqslant 2$

$$\forall m \in \{0, 1, 2, \ldots, n-1\} : \binom{n+m}{n} \equiv 1 \pmod{k}$$
$$\Longrightarrow k \in \mathcal{P} \text{ et } n = k^m \text{ pour un entier } m \geqslant 1.$$

En 1819, Babbage [2] prouve aussi que pour tout nombre premier $p \geqslant 3$, on a

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^2}.$$

En 1862, Wolstenholme [55] et [[16], p. 89] prouve que pour tout nombre premier $p \geqslant 5$, on a les deux congruences suivantes :

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}, \tag{1.2}$$
$$\sum_{k=1}^{p-1} \frac{1}{k} \equiv 0 \pmod{p^2}.$$

En 1895, Morley [39] prouve que pour tout nombre premier $p \geqslant 5$

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} \pmod{p^3}. \tag{1.3}$$

Remarquons que cette congruence implique la congruence suivante qui est facile à prouver directement :

$$\binom{p-1}{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \qquad p \geqslant 5. \tag{1.4}$$

La congruence (1.4) n'est pas un critère de primalité. Dans [1], Ayad et Kihel ont étudié les nombres impairs composés n vérifiant la congruence

$$\binom{n-1}{\frac{n-1}{2}} \equiv (-1)^{\frac{n-1}{2}} \pmod{n}.$$

Il ont trouvé que $n = 5907 = 3 \times 11 \times 179$ était le plus petit entier composé vérifiant cette congruence. Ils ont alors conjecturé que cette congruence n'admet pas de solutions n tels que n soit le produit de deux nombres premiers impairs.
En 1900, Glaisher [[12], p. 21], [[13], p. 323] prouve que pour tout entier $n \geqslant 1$, on a

$$\binom{np-1}{p-1} \equiv 1 \pmod{p^3}, \qquad p \geqslant 5 \tag{1.5}$$

$$\binom{np-1}{p-1} \equiv 1 - \frac{1}{3} n(n-1) p^3 B_{p-3} \pmod{p^4}, \qquad p \geqslant 5. \tag{1.6}$$

et que

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} \pmod{p^4} \quad p \geqslant 3.$$

En 1953, Carlitz [[8] et [9]] améliore la congruence de Morley en prouvant que

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1} + \frac{p^3}{12} B_{p-3} \pmod{p^4} \qquad p \geqslant 5.$$

En 1995, R. J. McIntosh [[30], p. 385] prouve que

$$\binom{2p-1}{p-1} \equiv 1 - p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} \pmod{p^5} \qquad p \geqslant 7. \tag{1.7}$$

En 2007, Zhao [58] prouve que

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} \pmod{p^5} \quad p \geqslant 7). \tag{1.8}$$

En 2010, Tauraso [49] prouve que

$$\binom{2p-1}{p-1} \equiv 1 + 2p \sum_{k=1}^{p-1} \frac{1}{k} + \frac{2}{3} p^3 \sum_{k=1}^{p-1} \frac{1}{k^3} \pmod{p^6} \qquad p \geqslant 7. \tag{1.9}$$

et

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} - 2p^2 \sum_{k=1}^{p-1} \frac{1}{k^2} \pmod{p^6} \qquad p \geqslant 7. \tag{1.10}$$

En 2014, Meštrović [36] prouve que

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} + 4p^2 \sum_{1 \leqslant i < j \leqslant p-1} \frac{1}{ij} \pmod{p^7} \qquad p \geqslant 11. \tag{1.11}$$

La congruence (1.11) a été encore généralisée par J. Rosen [45].

1.5 Enoncé du résultat principal

Le théorème suivant constitue à la fois une généralisation de la congruence de Wolstenholme et de la congruence de Morley ; en exploitant la relation suivante qui découle du lemme 1.22 :

$$(-1)^{\frac{p-1}{2}} \binom{p-1}{\frac{p-1}{2}} = 4^{p-1} \binom{\frac{1}{2}p-1}{p-1}. \tag{1.12}$$

Ce théorème permet aussi de retrouver toutes les généralisations des deux congruences que l'on a exposé au paragraphe précédent, et aussi d'en découvrir d'autres.

Théorème 1.14 ([4]). *Pour tout nombre premier $p > 2$ et pour tout p-entier α, on a*

$$\binom{\alpha p-1}{p-1} \equiv 1 - \alpha(\alpha-1)(\alpha^2-\alpha-1)p \sum_{k=1}^{p-1} \frac{1}{k} + \alpha^2(\alpha-1)^2 p^2 \sum_{1 \leqslant i < j \leqslant p-1} \frac{1}{ij} \pmod{p^m}. \tag{1.13}$$

où $m = 7$ si $p \neq 7$ et $m = 6$ si $p = 7$.

Avant de prouver ce théorème, donnons quelques corollaires de ce théorème
Pour $\alpha = 2$ et pour $\alpha = \frac{1}{2}$, le théorème 1.14 permet d'obtenir le corollaire suivant :

Corollaire 1.15. *Pour tout nombre premier impair p, on a*

$$\binom{2p-1}{p-1} \equiv 1 - 2p \sum_{k=1}^{p-1} \frac{1}{k} + 4p^2 \sum_{1 \leqslant i < j \leqslant p-1} \frac{1}{ij} \pmod{p^m} \tag{1.14}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1-\frac{5}{16}p\sum_{k=1}^{p-1}\frac{1}{k}+\frac{1}{16}p^2\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}\right) \pmod{p^m} \tag{1.15}$$

où $m=7$ si $p\neq 7$ et $m=6$ si $p=7$.

On constate ainsi que le théorème 1.14 est bien une généralisation des congruences de Wolstenholme (1.2) et de Morley(1.3). En effet, ces deux congruences se déduisent respectivement de (1.14) et (1.15) en observant qu'on a d'après (1.38) pour $m=1$ et (1.37) pour $m=2$

$$\sum_{k=1}^{p-1}\frac{1}{k}\equiv 0 \pmod{p^2} \text{ et } \sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}\equiv 0 \pmod{p}, \quad p\geqslant 5. \tag{1.16}$$

On déduit aussi du théorème 1.14 et de la relation (1.16) le corollaire suivant qui généralise aux p-entiers, la congruence de Glaisher (1.5).

Corollaire 1.16. *Pour tout p-entier α, on a*

$$\binom{\alpha p-1}{p-1}\equiv 1 \pmod{p^3}, \quad p\geqslant 5. \tag{1.17}$$

On déduit du théorème 1.14 les deux relations suivantes

$$\binom{2p-1}{p-1}\equiv 1-2p\sum_{k=1}^{p-1}\frac{1}{k}+4p^2\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij} \pmod{p^6}, \tag{1.18}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1-\frac{5}{16}p\sum_{k=1}^{p-1}\frac{1}{k}+\frac{1}{16}p^2\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}\right) \pmod{p^6}. \tag{1.19}$$

Comme on a

$$\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}=\frac{1}{2}\left(\sum_{k=1}^{p-1}\frac{1}{k}\right)^2-\frac{1}{2}\sum_{k=1}^{p-1}\frac{1}{k^2},$$

on en déduit de (1.16) *que*

$$p^2\sum_{1\leqslant i<j\leqslant p-1}\frac{1}{ij}\equiv -\frac{1}{2}p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^6}.$$

Compte tenu de cette dernière relation, on déduit encore du théorème 1.14 le corollaire suivant :

Corollaire 1.17. *Pour tout nombre premier impair p et pour tout p-entier α, on a*

$$\binom{\alpha p-1}{p-1}\equiv 1-\alpha(\alpha-1)(\alpha^2-\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k}-\frac{1}{2}\alpha^2(\alpha-1)^2p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^6} \tag{1.20}$$

Pour $\alpha=2$ et $\alpha=\frac{1}{2}$, ce corollaire nous fournit les deux relations suivantes

$$\binom{2p-1}{p-1}\equiv 1-2p\sum_{k=1}^{p-1}\frac{1}{k}-2p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^6}. \tag{1.21}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1-\frac{5}{16}p\sum_{k=1}^{p-1}\frac{1}{k}-\frac{1}{32}p^2\sum_{k=1}^{p-1}\frac{1}{k^2}\right) \pmod{p^6}. \tag{1.22}$$

De la relation (1.20) et du lemme 1.26, on déduit encore le corollaire suivant

Corollaire 1.18.

$$\binom{\alpha p-1}{p-1} \equiv 1-\frac{1}{3}\alpha(\alpha-1)p^3B_{p-3} \pmod{p^4} \tag{1.23}$$

La relation (1.23) est une généralisation de la congruence de Glaisher (1.6).
Pour $m=1$, la relation (1.43) implique

$$2p\sum_{k=1}^{p-1}\frac{1}{k}+p^2\sum_{k=1}^{p-1}\frac{1}{k^2}\equiv 0 \pmod{p^5} \quad p\geqslant 7. \tag{1.24}$$

On déduit de (1.22) et (1.20) le corollaire suivant

Corollaire 1.19. *Pour tout p-entier α, on a*

$$\binom{\alpha p-1}{p-1} \equiv 1+\alpha(\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k} \pmod{p^5} \qquad p\geqslant 7, \tag{1.25}$$

$$\binom{\alpha p-1}{p-1} \equiv 1-\frac{1}{2}\alpha(\alpha-1)p^2\sum_{k=1}^{p-1}\frac{1}{k^2} \pmod{p^5} \qquad p\geqslant 7. \tag{1.26}$$

Pour $\alpha=2$, la relation (1.26) permet de retrouver la congruence de R. J. McIntosh (1.7) et la relation (1.25) permet de retrouver la congruence de Zhao (1.8). De plus pour $\alpha=\frac{1}{2}$, les relations (1.21) et (1.22) nous fournissent le corollaire suivant :

Corollaire 1.20. *On a*

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1-\frac{1}{4}p\sum_{k=1}^{p-1}\frac{1}{k}\right) \pmod{p^5} \qquad p\geqslant 7, \tag{1.27}$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1+\frac{1}{8}p^2\sum_{k=1}^{p-1}\frac{1}{k^2}\right) \pmod{p^5} \qquad p\geqslant 7. \tag{1.28}$$

A l'aide de la relation (1.44) du lemme 1.25, écrite pour $m=1$, on déduit que l'on a

$$\sum_{k=1}^{p-1}\frac{1}{k}+\frac{1}{2}p\sum_{k=1}^{p-1}\frac{1}{k^2}+\frac{1}{6}p^2\sum_{k=1}^{p-1}\frac{1}{k^3}\equiv 0 \pmod{p^6} \qquad p\geqslant 11. \tag{1.29}$$

Avec (1.20) et (1.29), on déduit le corollaire suivant :

Corollaire 1.21. *Pour tout nombre premier impair $p\geqslant 11$ et pour tout p-entier α, on a*

$$\binom{\alpha p-1}{p-1} \equiv 1+\alpha(\alpha-1)p\sum_{k=1}^{p-1}\frac{1}{k}+\frac{1}{6}\alpha^2(\alpha-1)^2p^3\sum_{k=1}^{p-1}\frac{1}{k^3} \pmod{p^6}.$$

Pour $\alpha=2$ et $\alpha=\frac{1}{2}$, ce corollaire nous fournit les deux congruences suivantes vérifiées pour $p\geqslant 11$,

$$\binom{2p-1}{p-1} \equiv 1+2p\sum_{k=1}^{p-1}\frac{1}{k}+\frac{2}{3}p^3\sum_{k=1}^{p-1}\frac{1}{k^3} \pmod{p^6},$$

$$(-1)^{\frac{p-1}{2}}\binom{p-1}{\frac{p-1}{2}} \equiv 4^{p-1}\left(1-\frac{1}{4}p\sum_{k=1}^{p-1}\frac{1}{k}+\frac{1}{96}p^3\sum_{k=1}^{p-1}\frac{1}{k^3}\right) \pmod{p^6}.$$

Le théorème 1.14 généralise aux p-entiers, la relation (1.11) de Meštrović. Enfin pour prouver notre principal résultat qui est le théorème 1.14 , nous aurons besoin des lemmes suivants

1.6 Lemmes

Lemme 1.22. *Pour tout entier $n \geqslant 1$, on a*

$$(-1)^n\binom{2n}{n} = 4^{2n}\binom{n-\frac{1}{2}}{2n} \tag{1.30}$$

Démonstration. On a

$$\begin{aligned}
4^{2n}\binom{n-\frac{1}{2}}{2n} &= \frac{4^{2n}}{(2n)!}\prod_{k=1}^{2n}(n+\frac{1}{2}-k)\\
&= \frac{2^{2n}}{(2n)!}\prod_{k=1}^{2n}(2n+1-2k)\\
&= (-1)^n\frac{2^{2n}}{(2n)!}\prod_{k=1}^{n}(2\,(n+1-k)-1)\prod_{k=n+1}^{2n}(2(k-n)-1).
\end{aligned}$$

Ce qui peut s'écrire

$$4^{2n}\binom{n-\frac{1}{2}}{2n} = (-1)^n\frac{2^{2n}}{(2n)!}\left(\prod_{k=1}^{n}(2j-1)\right)^2. \tag{1.31}$$

On constate alors que

$$\prod_{k=1}^{n}(2j-1) = \frac{\prod_{j=1}^{n}(2j)\cdot\prod_{j=1}^{n}(2j-1)}{\prod_{j=1}^{n}(2j)} = \frac{(2n)!}{2^n n!} \tag{1.32}$$

Il résulte de (1.31) et (1.32) que

$$4^{2n}\binom{n-\frac{1}{2}}{2n} = (-1)^n\frac{2^{2n}}{(2n)!}\left(\frac{(2n)!}{2^n n!}\right)^2 = (-1)^n\frac{(2n)!}{n!n!} = (-1)^n\binom{2n}{n}.$$

□

En chosissant $n = \frac{p-1}{2}$ dans (1.30), on obtient la relation (1.12).

Pour tout nombre premier p et pour tout entier k, nous définissons les nombres harmoniques généralisés H_m par

$$H_m = \sum_{1\leqslant k_1<\ldots<k_m\leqslant p-1}\frac{1}{k_1\ldots k_m}, \qquad \text{pour } 1\leqslant m\leqslant p-1.$$

Par convention, on pose :

$$H_0 = 1 \text{ et } H_m = 0 \text{ pour } m \geqslant p. \tag{1.33}$$

Soit $P(x)$ le polynôme défini par

$$P(x) = \frac{(x-1)(x-2)\dots(x-p+1)}{(p-1)!}, \tag{1.34}$$

on a alors

$$P(x) = (-1)^{p-1} \prod_{k=1}^{p-1} \frac{k-x}{k} = \prod_{k=1}^{p-1} \left(1 - \frac{x}{k}\right).$$

On en déduit que

$$P(x) = \sum_{k=0}^{p-1} (-1)^k H_k x^k. \tag{1.35}$$

La preuve du théorème principal repose essentiellement sur le lemme suivant

Lemme 1.23. *Pour tout nombre premier p impair et pour tout entier $m \geqslant 1$, on a*

1.

$$H_{2m-1} - mpH_{2m} = \frac{1}{2}p^2 \sum_{k=2m+1}^{p-1} (-1)^k \binom{k}{2m-1} p^{k-2m-1} H_k, \tag{1.36}$$

2.

$$H_m \equiv 0 \pmod{p}, \text{ pour } m \neq p-1, \tag{1.37}$$

3.

$$H_m \equiv 0 \pmod{p^2}, \text{ pour } m \text{ impair et } m \neq p-2, \tag{1.38}$$

4.

$$H_{2m-1} - mpH_{2m} \equiv 0 \pmod{p^4}, \text{ pour } 2m+1 \neq p-2. \tag{1.39}$$

Démonstration. 1. La relation (1.34) nous permet de constater que l'on a

$$P(x) = P(p-x),$$

ce qui peut s'écrire, en exploitant la relation (1.35) et la convention (1.33) :

$$\sum_{k\geqslant 0} (-1)^k H_k x^k = \sum_{k\geqslant 0} (-1)^k H_k (p-x)^k. \tag{1.40}$$

En identifiant les coefficients de x^{2m-1} dans chacun des deux membres de (1.40), on obtient

$$\begin{aligned} -H_{2m-1} &= \sum_{k\geqslant 0} (-1)^k H_k \binom{k}{2m-1} p^{k-2m+1} (-1)^{2m-1} \\ &= -\sum_{k=2m-1}^{p-1} (-1)^k \binom{k}{2m-1} p^{k-2m+1} H_k \\ &= H_{2m-1} - 2mpH_{2m} - p^2 \sum_{k=2m+1}^{p-1} (-1)^k \binom{k}{2m-1} p^{k-2m-1} H_k. \end{aligned}$$

La relation (1.36) en résulte. Remarquons qu'on déduit de cette relation que $H_{2m-1} \equiv 0 \pmod{p}$ pour tout $m \geqslant 1$.

2. Il s'agit d'un résulat bien connu qu'on peut déduire facilement du fait que le polynôme $P(x)$ considéré comme un polynôme à coefficients dans le corps $\mathbb{Z}/p\mathbb{Z}$ s'écrit grâce au petit théorème de Fermat $P(x) = 1 - x^{p-1}$. On en déduit aussi que $H_{p-1} = \frac{1}{(p-1)!} \equiv -1 \pmod{p}$.

3. D'après la relation (1.36), on a

$$H_{2m-1} \equiv mpH_{2m} \pmod{p^2}. \tag{1.41}$$

On a alors $H_{2m-1} \equiv 0 \pmod{p^2}$ pour $2m-1 \neq p-2$ car on a $H_{2m} \equiv 0 \pmod{p}$ d'après (1.37). Remarquons que si $2m-1 = p-2$, on a $H_{2m-1} = H_{p-2} \equiv \frac{p-1}{2} pH_{p-1} \equiv \frac{p}{2} \pmod{p^2}$.

4. D'après la relation (1.36), on a

$$H_{2m-1} - mpH_{2m} \equiv -\frac{1}{2}p^2\binom{2m+1}{2}H_{2m+1} + \frac{1}{2}p^3\binom{2m+2}{3}H_{2m+2} \pmod{p^4}. \tag{1.42}$$

Si $2m+1 \neq p-2$, on a alors $2m+2 \neq p-1$ et on déduit de (1.38) et (1.37) que $H_{2m+1} \equiv 0 \pmod{p^2}$ et $H_{2m+2} \equiv 0 \pmod{p}$. En tenant compte de ces deux dernières congruences dans (1.42), la relation (1.39) en résulte.

□

Remarque 1.24. *Il est facile de prouver à l'aide de la relation (1.42) que si* $2m+1 = p-2$, *alors* .

$$H_{2m-1} - mpH_{2m} = H_{p-4} - \left(\frac{p-3}{2}\right)pH_{p-3} \equiv -\frac{p^3}{4} \pmod{p^4}.$$

Ainsi, pour tout $m \geqslant 1$, *on a* $H_{2m-1} - mpH_{2m} \equiv 0 \pmod{p^3}$.

Lemme 1.25. *Pour tout entier* $m \geqslant 1$, *on a*

1.

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \begin{cases} 0 \pmod{p} & si\ p-1 \nmid m \\ -1 \pmod{p} & si\ p-1 \mid m \end{cases}.$$

2.

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \begin{cases} 0 \pmod{p^2} & si\ m\ est\ impair\ et\ p-1 \nmid m+1 \\ \frac{1}{2}mp \pmod{p^2} & si\ m\ est\ impair\ et\ p-1 \mid m+1 \end{cases}.$$

3. Pour m *impair, on a*

$$2\sum_{k=1}^{p-1} \frac{1}{k^m} + mp\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} \equiv \begin{cases} 0 \pmod{p^3} & \\ 0 \pmod{p^4} & si\ p-1 \nmid m+3 \\ -\frac{1}{12}m(m+1)(m+2)p^3 \pmod{p^4} & si\ p-1 \mid m+3 \end{cases} \tag{1.43}$$

4. Pour m *impair, si* $p-1 \nmid m+5$ *on a*

$$\sum_{k=1}^{p-1} \frac{1}{k^m} + \frac{1}{2}mp\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} + \frac{m(m+1)}{12}p^2\sum_{k=1}^{p-1} \frac{1}{k^{m+2}} \equiv 0 \pmod{p^6} \tag{1.44}$$

Démonstration. 1. Soit $g \in \mathbb{Z}$ tel que $\overline{g}$ soit un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^*$. L'application $x \longmapsto x^{-1}$ de $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui-même étant bijective, on a

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \sum_{k=1}^{p-1} k^m \equiv \sum_{j=0}^{p-2} \left(g^j\right)^m \equiv \sum_{j=0}^{p-2} (g^m)^j \equiv 0 \pmod{p}.$$

On a alors

$$(g^m-1)\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv (g^m-1)\sum_{j=0}^{p-2} (g^m)^j = (g^m)^{p-1} - 1 = \left(g^{p-1}\right)^m - 1 \equiv 0 \pmod{p}.$$

On en déduit que si $p-1 \nmid m$, on a $g^m - 1 \not\equiv 0 \pmod p$ et

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv 0 \pmod p.$$

Si $p-1 \mid m$, on a $\frac{1}{k^m} \equiv 1 \pmod p$ pour $1 \leqslant k \leqslant p-1$ et

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \sum_{k=1}^{p-1} 1 = p-1 \equiv -1 \pmod p.$$

2. Pour m impair, on a

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{1}{k^m} &= \frac{1}{2}\sum_{k=1}^{p-1} \frac{1}{k^m} + \frac{1}{2}\sum_{k=1}^{p-1} \frac{1}{(p-k)^m} \\ &= \frac{1}{2}\sum_{k=1}^{p-1} \frac{(p-k)^m + k^m}{k^m(p-k)^m} \equiv -\frac{1}{2}mp\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} \pmod{p^2}. \end{aligned} \tag{1.45}$$

Si $p-1 \nmid m+1$, on a

$$\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} \equiv 0 \pmod p$$

et (1.45) implique

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv 0 \pmod{p^2}.$$

Si $p-1 \mid m+1$; alors

$$\sum_{k=1}^{p-1} \frac{1}{k^{m+1}} \equiv -1 \pmod p$$

et (1.45) implique

$$\sum_{k=1}^{p-1} \frac{1}{k^m} \equiv \frac{1}{2}mp \pmod{p^2}.$$

3. On a pour $1 \leqslant k \leqslant p-1$

$$\begin{aligned} \frac{1}{\left(1-\frac{p}{k}\right)^m} \equiv 1 + m\frac{p}{k} + \binom{m+1}{2}\frac{p^2}{k^2} + \binom{m+2}{3}\frac{p^3}{k^3} \\ + \binom{m+3}{4}\frac{p^4}{k^4} + \binom{m+4}{5}\frac{p^5}{k^5} \pmod{p^6}. \end{aligned}$$

On en déduit que pour m impair, on a

$$\sum_{k=1}^{p-1}\frac{1}{(p-k)^m}\equiv-\sum_{k=1}^{p-1}\frac{1}{k^m}-\sum_{k=1}^{p-1}\frac{mp}{k^{m+1}}$$
$$-\binom{m+1}{2}\sum_{k=1}^{p-1}\frac{p^2}{k^{m+2}}-\binom{m+2}{3}\sum_{k=1}^{p-1}\frac{p^3}{k^{m+3}}$$
$$-\binom{m+3}{4}\sum_{k=1}^{p-1}\frac{p^4}{k^{m+4}}-\binom{m+4}{5}\sum_{k=1}^{p-1}\frac{p^5}{k^{m+5}}\pmod{p^6}.$$

Il en résulte que

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}+mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}\equiv-\tbinom{m+1}{2}p^2\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}-\tbinom{m+2}{3}p^3\sum_{k=1}^{p-1}\frac{1}{k^{m+3}}$$
$$-\tbinom{m+3}{4}p^4\sum_{k=1}^{p-1}\frac{1}{k^{m+4}}-\tbinom{m+4}{5}p^5\sum_{k=1}^{p-1}\frac{1}{k^{m+5}}\pmod{p^6}.\quad(1.46)$$

Or $m+2$ est impair. On a donc $p-1\nmid m+2$ et

$$\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}\equiv 0\pmod{p}.$$

On déduit alors de (1.46) que

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}+mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}\equiv 0\pmod{p^3}.$$

Si $p-1\nmid m+3$, on a à la fois

$$\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}\equiv 0\pmod{p^2}\quad\text{et}\quad\sum_{k=1}^{p-1}\frac{1}{k^{m+3}}\equiv 0\pmod{p}.$$

La relation (1.46) montre que

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}\equiv-mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}\pmod{p^4}.$$

Si $p-1\mid m+3$, on a

$$\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}\equiv\frac{1}{2}(m+2)p\pmod{p^2}\quad\text{et}\quad\sum_{k=1}^{p-1}\frac{1}{k^{m+3}}\equiv-1\pmod{p}.$$

On obtient toujours d'aprés (1.46) que :

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}+mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}} \equiv -\frac{m(m+1)(m+2)}{4}p^3+\frac{m(m+1)(m+2)}{6}p^3$$
$$\equiv -\frac{1}{12}m(m+1)(m+2) \pmod{p^4}.$$

4. Si m impair et si $p-1 \nmid m+5$, alors

$$\sum_{k=1}^{p-1}\frac{1}{k^{m+5}}\equiv 0 \pmod{p}, \quad \sum_{k=1}^{p-1}\frac{1}{k^{m+4}}\equiv 0 \pmod{p^2}$$

Par suite

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}\equiv -mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}-\frac{m(m+1)}{2}p^2\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}$$
$$-\frac{m(m+1)(m+2)}{6}p^3\sum_{k=1}^{p-1}\frac{1}{k^{m+3}} \pmod{p^6}. \quad (1.47)$$

On a aussi d'après (1.43)

$$2p^2\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}+(m+2)p^3\sum_{k=1}^{p-1}\frac{1}{k^{m+3}}\equiv 0 \pmod{p^6}. \quad (1.48)$$

On déduit de (1.47) et (1.48)

$$2\sum_{k=1}^{p-1}\frac{1}{k^m}\equiv -mp\sum_{k=1}^{p-1}\frac{1}{k^{m+1}}-\frac{m(m+1)}{2}p^2\sum_{k=1}^{p-1}\frac{1}{k^{m+2}}$$
$$+\frac{m(m+1)}{3}p^2\sum_{k=1}^{p-1}\frac{1}{k^{m+2}} \pmod{p^6}.$$

La relation (1.44) en résulte. □

Lemme 1.26. *On a*

$$\sum_{k=1}^{p-1}\frac{1}{k} \equiv -\frac{1}{3}p^2B_{p-3} \pmod{p^3}, \qquad p\geqslant 5 \quad (1.49)$$

$$\sum_{k=1}^{p-1}\frac{1}{k^2} \equiv \frac{2}{3}pB_{p-3} \pmod{p^2}, \qquad p\geqslant 5. \quad (1.50)$$

On trouvera dans [19] une preuve trés détaillée de la relation (1.49) qui est un résultat dû à Glaisher [12]. La relation (1.50) se déduit de (1.49) et de (1.43) écrite pour $m=1$.

1.7 Preuve du théorème 1.14

D'après la relation (1.35), on a

$$\binom{\alpha p-1}{p-1} = P(\alpha p) = \sum_{k=0}^{p-1} (-\alpha)^k H_k p^k.$$

On en déduit que

$$\binom{\alpha p-1}{p-1} = \sum_{k=0}^{4} (-\alpha)^k H_k p^k + (-\alpha)^5 H_5 p^5 + (-\alpha)^6 H_6 p^6 \pmod{p^7}. \tag{1.51}$$

Or, d'après les relations (1.37) et (1.38), on a

$$(-\alpha)^5 H_5 p^5 \equiv 0 \pmod{p^7} \text{ et } (-\alpha)^6 H_6 p^6 \equiv 0 \pmod{p^7}, \tag{1.52}$$

pourvu que $5 \neq p-2$ et $6 \neq p-1$, c'est à dire $p \neq 7$. Il suffit donc de choisir $p \geqslant 11$ pour réaliser ces conditions.
Ainsi pour $p \geqslant 11$, il résulte des relations (1.51) et (1.52) que l'on a

$$\binom{\alpha p-1}{p-1} \equiv \sum_{k=0}^{4} (-\alpha)^k H_k p^k \pmod{p^7}. \tag{1.53}$$

Pour $\alpha = 1$, nous déduisons de (1.53) la relation

$$\sum_{k=1}^{4} (-\alpha)^k H_k p^k \equiv 0 \pmod{p^7}. \tag{1.54}$$

D'autre part, du fait que $p \geqslant 11$, on a d'après (1.39) du lemme 1.23,

$$p^3 H_3 - 2p^4 H_4 \equiv 0 \pmod{p^7}. \tag{1.55}$$

Des relations (1.53), (1.54) et (1.55), on déduit que pour tous p-entiers λ et μ, on a

$$\binom{\alpha p-1}{p-1} \equiv \sum_{k=0}^{4} (-\alpha)^k H_k p^k + \lambda \left(\sum_{k=1}^{4} (-\alpha)^k H_k p^k \right) + \mu \left(p^3 H_3 - 2p^4 H_4 \right) \pmod{p^7}. \tag{1.56}$$

Autrement dit, on a

$$\binom{\alpha p-1}{p-1} \equiv \sum_{k=0}^{4} A_k H_k p^k \pmod{p^7},$$

avec

$$\begin{aligned} A_0 &= 1, \\ A_1 &= -\alpha - \lambda, \\ A_2 &= \alpha^2 + \lambda, \\ A_3 &= -\alpha^3 - \lambda + \mu \\ A_4 &= \alpha^4 + \lambda - 2\mu. \end{aligned}$$

Choisissons λ et μ tels que $A_3 = A_4 = 0$, on obtient

$$\lambda = \alpha^4 - 2\alpha^3 \quad \text{et} \quad \mu = \alpha^4 - \alpha^3.$$

Avec ce choix de λ et μ, la relation (1.56) devient

$$\binom{\alpha p - 1}{p-1} \equiv 1 - (\alpha^4 - 2\alpha^3 + \alpha) p H_1 + (\alpha^4 - 2\alpha^3 + \alpha^2) p^2 H_2 \pmod{p^7}.$$

Ce qui nous fournit bien la relation (1.13).
Si $p = 7$, un calcul direct donne

$$\binom{\alpha p - 1}{p-1} - \left(1 - \alpha(\alpha-1)(\alpha^2-\alpha-1)p \sum_{k=1}^{p-1} \frac{1}{k} + \alpha^2(\alpha-1)^2 p^2 \sum_{1 \leqslant i < j \leqslant p-1} \frac{1}{ij}\right)$$
$$= \frac{\alpha^3(\alpha-1)^3}{720} 7^6 \equiv 0 \pmod{7^6}$$

et permet de conclure. La preuve du théorème est complète.

Théorème 1.27. *Pour tout nombre premier $p \geqslant 11$ et tout p-entier α on a*

$$\binom{\alpha p - 1}{p-1} \equiv 1 + (\alpha^2 - \alpha)(2\alpha^4 - 4\alpha^3 + \alpha^2 + \alpha + 1) p H_1$$
$$- \alpha^2(\alpha-1)^2(2\alpha^2 - 2\alpha - 1) p^2 H_2 + \alpha^3(\alpha-1)^3 H_3 \pmod{p^9}.$$

Démonstration. En utilisant la même méthode que dans la preuve du théorème 1.14, on peut avoir une congruence pour $\binom{\alpha p-1}{p-1}$ modulo p^9, similaire à 1.14, faisant intervenir H_1, H_2, H_3 et H_4. En exploitant le fait que $\binom{-p-1}{p-1} = \binom{2p-1}{p-1}$, on obtient $p^4 H_4 \equiv 5pH_1 - 5p^2 H_2 + 3p^3 H_3 \pmod{p^9}$, cette dernière relation nous permettra d'éliminer H_4 et obtenir la congruence souhaitée. □

Pour $\alpha = 2$, on obtient la congruence de Rosen [44] suivante

Corollaire 1.28. *pour tout nombre premier $p \geqslant 11$ on a*

$$\binom{2p-1}{p-1} \equiv 1 + 14pH_1 - 12p^2 H_2 + 8p^3 H_3 \pmod{p^9}. \tag{1.57}$$

Chapitre 2

Etude de certaines équations diophantiennes quadratiques

"Dieu créa le nombre entier tout le reste est l'œuvre de l'homme"
Leopold Kronecker

2.1 Généralités sur les équations diophantiennes

2.1.1 Introduction

Une équation diophantienne est une équation de la forme

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

où f est une fonction donnée et pour laquelle on cherche les solutions $(x_1, x_2, \ldots, x_n)$ entières ou rationnelles. En général, $f(x_1, x_2, \ldots, x_n)$ est un polynôme à coefficients rationnels. On peut aussi s'intéresser aux solutions entières ou rationnelles d'un système d'équations polynomiales à coefficients rationnels. Les questions suivantes sont naturelles et fondamentales :

— L'équation (ou le système d'équations) admet-elle des solutions ?
— Le nombre de solutions est-il fini ou non ?
— Est-il possible de déterminer toutes les solutions ?

2.1.2 Un peu d'histoire

L'étude des équations diophantiennes remonte à l'antiquité, elles furent introduites et étudiées pour la première fois par le mathématicien grec Diophante d'Alexandrie ($325-409$). En fait, l'époque à laquelle il vécut à Alexandrie est incertaine. Les historiens la situent entre le deuxième siècle av. J.-C. et le cinquième siècle et vraisemblablement au quatrième siècle. Diophante a écrit plusieurs ouvrages mathématiques, le plus célèbre est certainement son traité "les Arithmétiques" qui comprend treize livres avec 280 problèmes. De son œuvre constituée de ces treize ouvrages d'arithmétique, écrits en grec, seulement six étaient connus jusqu'en 1968. La traduction en Latin de l'œuvre de Diophante par Bachet date de 1621. En 1968, une traduction en arabe fut découverte en Iran. Il s'agissait de quatre nouveaux livres de Diophante, en arabe, traduits du grec, et écrits à Alexandrie probablement par un des commentateurs de Diophante. Regiomontanus [7] traduit : Citons, à titre d'exemple, le problème suivant :

"Trouver quatre nombres a, b, c, d tels que le produit de deux d'entre eux augmenté de 1 soit un carré parfait, les nombres en question étant des nombres rationnels", autrement dit, on cherche quatre nombres rationnels (distincts) a, b, c, d tels que les nombres rationnels $ab+1$, $ac+1$, $ad+1$,

$bc+1$, $bd+1$, $cd+1$ soient tous des carrés dans $\mathbb{Q}$. Un quadruplet (a,b,c,d) ayant cette propriété est appelé un quadruplet diophantien rationnel, ainsi,

$$(a,b,c,d)=\left(\frac{1}{16},\frac{33}{16},\frac{17}{4},\frac{105}{16}\right)$$

est un quadruplet diophantien puisque

$$\begin{aligned}
\frac{1}{16}\cdot\frac{33}{16}+1 &= \left(\frac{17}{16}\right)^2\\
\frac{1}{16}\cdot\frac{17}{4}+1 &= \left(\frac{9}{8}\right)^2\\
\frac{1}{16}\cdot\frac{105}{16}+1 &= \left(\frac{19}{16}\right)^2\\
\frac{33}{16}\cdot\frac{17}{4}+1 &= \left(\frac{25}{8}\right)^2\\
\frac{33}{16}\cdot\frac{105}{16}+1 &= \left(\frac{61}{16}\right)^2\\
\frac{17}{4}\cdot\frac{105}{16}+1 &= \left(\frac{43}{8}\right)^2.
\end{aligned}$$

On trouve dans l'ouvrage de Hawking décédé recemment ([17])ou de S. Tengely ([50]) un important extrait des six livres Arithmétiques et du livre des nombres polygones (p. 217−306). Signalons qu'on attribue à la mathématicienne Hypatie d'Alexandrie, qui est née aux environs de 360 après. J.-C. et qui connut une fin tragique, la rédaction de commentaires sur les *Arithmétiques* de Diophante. Quelques siècles après l'époque où vécut Diophante, les Arabo-musulmans traduisirent et développèrent les œuvres de Diophante ; on peut citer par exemple, au VIII siècle, Abu l'wafa (940 - 998) un mathématicien perse, Qusta ibn luqa (820–912) de Baalabek qui traduisa les *Arithmétiques,* ainsi que les mathématiciens du IX-ième et X-ième siècles, Al-karaji (953–1029), Alkhazin (900–971), qui étudièrent les équations de Diophante et réalisérent une avancée importante. L'école indienne de l'époque, elle aussi participa activement à perpétuer l'oeuvre de Diophante. Mais il faut attendre la renaissance avec les travaux de Bachet de Méziriac (1581–1638) pour voir l'oeuvre de Diophante vulgarisée en Europe. Le véritable déclic a eu lieu avec Fermat, Lagrange, Dirichlet et Euler. Grâce à ces derniers, les méthodes utilisées pour résoudre ces équations prirent un aspect arithmétique plus rigoureux.

Lors du deuxième congrès international des mathématiciens, tenu à Paris en 1900, David Hilbert (1862–1943) présenta une liste de problèmes qui tenaient jusqu'alors les mathématiciens en échec ; ces problèmes devraient, selon Hilbert, marquer le cours des mathématiques du XX-ième siècle ; et on peut dire aujourd'hui que cela a été grandement le cas. Publiée après la tenue du congrès, la liste définitive comprenait 23 problèmes, aujourd'hui appelés les problèmes de Hilbert.

Le dixième problème pose la question suivante : existe-t-il un algorithme général permettant de déterminer si une équation diophantienne quelconque $P(x,y,z,\ldots)=0$ admet une solution en nombres entiers ?

Le problème a été résolu par Yuri Matiyasevitch [33] en 1970 ; dans ses travaux, il montra l'impossibilité de trouver une méthode qui résout toutes les équations diophantiennes, ce qui laisse le champ ouvert pour l'étude des équations diophantiennes particulières.

La recherche d'une solution d'une équation diophantienne comme celle du grand théorème de Fermat a donné naissance aux nombres algèbriques et au développement de la théorie algébrique des corps de nombres par Kummer, Dirichlet, Dedekind et Wiles...

Le lien entre les équations diophantiennes, les congruences, les courbes elliptiques, les courbes mo-

dulaires et la cryptographie n'est plus à démontrer. Plus encore, de ces équations diophantiennes ont découlé de nouvelles théories mathématiques, telles que l'analyse diophantienne, les approximations diophantiennes et la géométrie diophantienne.

Parmi les équations diophantiennes, ou des problèmes diophantiens en général, qui ont marqué l'histoire des mathématiques on peut citer :

— L'équation de Pythagore $(-570, -490)$: $x^2 + y^2 = z^2$:
Les solutions sont dites triplets pythagoriciens $(\pm dx_0, \pm dy_0, \pm dz_0)$ où d est un entier et $(x_0, y_0, z_0) = (m^2 - n^2, 2mn, m^2 + n^2)$.

— L'équation de Fermat (1601–1665) $x^n + y^n = z^n \quad (n \geqslant 3)$:

Il ne serait pas exagéré de dire que c'est la plus célèbre, sans aucun doute, des équations diophantiennes, voire des problèmes mathématiques. Ce défi mathématique a resisté plus de 350. En 1995, Andrew Wiles (1953−), avec l'assistance de son étudiant Richard Taylor (1962−), donna une preuve du théorème de Fermat, c'est-à-dire que l'équation $x^n + y^n = z^n \quad (n \geqslant 3)$ n'a pas de solutions avec x, y, z des entiers non tous nuls).

— L'équation d'Euler (1707–1783) : $x^4 + y^4 + z^4 = w^4$.

— L'équation de Catalan (1814–1894) : $x^m - y^n = 1.(n, m \geqslant 2)$

— L'équation de Pell (1611–1685) : $x^2 - Dy^2 = 1$.

— L'équation de Bachet (1581–1638) : $x^2 = y^3 + k$ $(k \in \mathbb{Z})$.

— L'équation de Hurwitz (1859-1919) : $x_1^2 + x_2^2 + \cdots + x_n^2 = kx_1x_2 \cdots x_n \quad (n \geqslant 2, k \in \mathbb{N}^*)$.

— L'équation de Ramanujuan (1887–1920)-Nagell (1895–1988) : $x^2 - d = p^n$ ($d < 0$, $n \in \mathbb{N}$, p un nombre premier).

2.2 Fractions continues

Les fractions continues sont trés usitées pour l'approximation des irrationnels par des rationnels, ainsi que pour l'étude de la transcendance ; elles restent l'outil principal pour le calcul des solutions fondamentales des équations de Pell. Pou cela, nous rappelons quelques propriétés des fractions continues.

On appelle fraction continue simple toute expression de la forme

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

où $a_0 \in \mathbb{Z}$, et pour $n \geqslant 1$, $a_n \in \mathbb{N}^*$ et que l'on note $[a_0; a_1, \ldots, a_n, ...]$. Elle peut être finie ou infinie.

Tout nombre réel est développable en fraction continue.

En effet, soit x un réel, alors on peut écrire $x = a_0 + t_0$ avec $a_0 = [x]$ et $0 \leqslant t_0 < 1$.

Si $t_0 = 0$, l'algorithme s'arrête, si $t_0 \neq 0$, alors $x = a_0 + \frac{1}{\frac{1}{t_0}}$ avec $a_0 \in \mathbb{Z}$ et $\dfrac{1}{t_0} > 1$.

$\dfrac{1}{t_0} = a_1 + t_1$ avec $a_1 = \left[\dfrac{1}{t_0}\right] \in \mathbb{N}$ et $0 \leqslant t_1 < 1$ de telle sorte que

$$x = a_0 + \frac{1}{a_1 + t_1}.$$

Si $t_1 = 0$, l'algorithme s'arrête. Si $t_1 \neq 0$, alors $\frac{1}{t_1} = a_2 + t_2$ avec $a_2 = \left[\dfrac{1}{t_1}\right]$ et $0 \leqslant t_2 < 1$ de telle

sorte que

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + t_2}}.$$

De cette manière, si $t_n \neq 0$, $\dfrac{1}{t_n} = a_{n+1} + t_{n+1}$ avec $a_{n+1} \in \mathbb{N}$ et $0 \leqslant t_{n+1} < 1$. Ainsi on obtient

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \quad a_n + \cfrac{1}{a_{n+1} + t_{n+1}}}}} = [a_0; a_1 \ldots, a_n, a_{n+1} + t_{n+1}]$$

La proposition suivante n'est pas dificile à prouver

Proposition 2.1 ([56]). *Soient les deux suites définies par $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$, et pour tout $n \geqslant 1$,*

$$p_n = a_n p_{n-1} + p_{n-2} \quad et \quad q_n = a_n q_{n-1} + q_{n-2}$$

alors on a

- $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n-1}$.
- $p_n q_{n-1} - q_n p_{n-2} = (-1)^n a_n$.
- $[a_0; a_1, \ldots, a_n] = \frac{p_n}{q_n}$ et $\operatorname{pgcd}(p_n, q_n) = 1$.
- la suite $C_{2n} = [a_0; a_1, \ldots, a_{2n}]$ est croissante, la suite $C_{2n+1} = [a_0; a_1, \ldots, a_{2n+1}]$ est décroissante.

$\frac{p_n}{q_n}$ est appelée n-ième réduite de la fraction continue la suite $\left(\frac{p_n}{q_n}\right)_{n \geqslant 0}$ est convergente vers x.

Une fraction continue est finie si et seulement si elle représente un nombre rationnel [56].

Une fraction continue $[a_0; a_1, a_2, \ldots, a_n \ldots]$ est dite périodique de période ℓ, s'il existe $\ell \geqslant 1$ tel que $a_k = a_{k+\ell}$ pour tout $k \geqslant n_0$; autrement dit, la fraction continue est de la forme

$$[a_0; a_1, \ldots, a_{n_0-1}, a_{n_0}, a_{n_0+1}, \ldots, a_{n_0+\ell-1}, a_{n_0}, a_{n_0+1}, \ldots, a_{n_0+\ell-1}, \ldots]$$

dans ce cas, la fraction continue est notée

$$[a_0; a_1, \ldots, a_{n_0-1}, \overline{a_{n_0}, a_{n_0+1}, \ldots, a_{n_0+\ell-1}}]$$

une fraction continue est dite purement périodique si elle est de la forme

$$[\overline{a_0; a_1, a_2, \ldots, a_{n_0}}]$$

pour un certain n_0.

Rappelons quelques propriétés du développement en fraction continue d'un nombre quadratique.

n sait que un réel α est dit nombre algèbrique s'il est racine d'un polynôme non nul $P(X) \in \mathbb{Q}[X]$; l'ensemble de ces polynômes est un idéal pricipal I_α de $\mathbb{Q}[X]$ engendré par un polynôme unitaire $P_\alpha(X) \in I_\alpha$, ce polynôme est appelé polynôme minimal de α, et son degré est appelé degré de α. Un nombre algèbrique réel de degré deux est dit nombre quadratique. Le théorème suivant, caractérise les nombres irrationnels quadratiques moyennant leurs développements en fractions continues.

Théorème 2.2 (Lagrange [56]). *Une fraction continue est périodique si et seulement si elle représente un nombre irrationnel quadratique. Si d est un entier positif qui n'est pas un carré parfait,*

alors le développement en fraction continue de $\sqrt{d}$ *est* $\left[a_0; \overline{a_1, a_2, \ldots, a_{\ell-1}, 2a_0}\right]$ *où* $a_0 = \left[\sqrt{d}\right]$ *et*

$$\begin{array}{ll} (a_1, a_2, \ldots, a_{\ell-1}) = (a_1, a_2, \ldots, a_j, a_j, \ldots, a_2, a_1) & \text{si } \ell = 2j+1. \\ (a_1 a_2 \ldots a_{\ell-1}) = (a_1, a_2, \ldots a_{j-1}, a_j, a_{j-1}, \ldots, a_2, a_1) & \text{si } \ell = 2j. \end{array}$$

Exemple 2.3. *Soit* $d = 5$
$a_0 = \left[\sqrt{5}\right] = 2$, $t_1 = \frac{1}{t_0 - a_0} = \frac{1}{\sqrt{5}-2} = \sqrt{5}+2$ *et* $a_1 = \left[\sqrt{t_1}\right] = 4$
$t_2 = \frac{1}{t_1 - a_1} = \frac{1}{\sqrt{5}-2} = t_1$ *et* $a_2 = \left[\sqrt{t_2}\right] = a_1$.
Ainsi on obtient $t_n = t_1$ *et* $a_n = a_1$ *pour tout* $n \geqslant 1$. *Par suite*

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

Soit $\alpha = a + b\sqrt{d} \in \mathbb{R}$, un irrationel quadratique et $\overline{\alpha} = a - b\sqrt{d}$ son conjugué, α est dit réduit si $\alpha > 1$ et $-1 < \overline{\alpha} < 0$.

Exemple 2.4. $1+\sqrt{2}$, $1+\sqrt{3}$ *sont réduits.*
Le développement en fraction continue de $1+\sqrt{2}$ *est purement périodique :*

$$1 + \sqrt{2} = 2 + \frac{1}{\sqrt{2}+1} = \left[\overline{2}\right].$$

En fait dès qu'un nombre algèbrique α est de degré $n > 2$, on ne sait pas grand chose sur son développement en fraction continue tels que : périodicité, lien des éléments du développement avec le degré n, et ordre de grandeur des élements du développement.

2.3 Equation de Pell

Pour démontrer les théorèmes figurant dans nous avons besoin de résultats concernant l'équation de Pell

2.3.1 Généralités

On appelle équation de Pell, ou parfois de Pell-Fermat, l'équation diophantienne $x^2 - dy^2 = 1$, où d est un entier positif fixé non carré parfait et les inconnues x, y sont des entiers positifs (les solutions dans $\mathbb{Z}$ étant obtenues en changeant les signes des solutions positives). Cette équation a passionné pendant des siècles, et passionne encore, des générations de mathématiciens ; il est bien connu que le premier exemple de cette équation trouve son origine à l'époque d'Archimède (-287, -212) où la determination de la taille d'un troupeau (troupeau d'Hélios, Dieu soleil) composé de boeufs et vaches de couleur blanche, noire, brune et tachetée, revient aprés formulation mathématique à résoudre l'équation $x^2 - 410286423278424y^2 = 1$.(voir [26]).

Les mathématiciens s'accordent à dire que le mathématicien anglais Brouncker (1620-1684) fut le premier à donner des méthodes rigoureuses pour la résolution de l'équation de Pell. Puis vint Lagrange (1736-1813). La dite équation de Pell a été aussi étudiée, indépendamment des mathématiciens européens, par les mathématiciens indiens Brahmagupta (598-670) pour $d = 92$, Bhaskara (1114-1185) pour $d = 61$. L'équation a été attribuée par Euler à Pell bien que, à l'unanimité des historiens des mathématiques, Pell n'a apporté aucune contribution à la résolution de cette équation ; l'apport de Pell s'est fait dans d'autres domaines de mathématiques. L'importance de cette équation réside dans le fait qu'elle a un lien étroit avec l'équation diophantienne quadratique générale

$$ax^2 + by^2 + cxy + dx + ey + f = 0 \quad (a, b, c, d, e, f \in \mathbb{Z}).$$

Désignons par D l'ensemble des entiers naturels qui ne sont pas des carrés

$$D = \mathbb{N} - \left\{n^2 \ / \ n \in \mathbb{N}\right\} = \{2, 3, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 17, \ldots\}\,.$$

Si on ordonne dans l'ordre croissant les éléments de D et si on désigne par d_n le n-ième élément de D, alors la suite $(d_n)_{n\geqslant 1}$ est répertoriée dans l'encyclopédie Sloane des suites en ligne [47] sous la référence $A000037$. On a la formule suivante, à la fois simple et curieuse :

$$d_n = n + \left[\frac{1}{2} + \sqrt{n}\right].$$

Soit d un entier strictement positif qui ne soit pas un carré parfait et C un entier non nul. L'équation diophantienne

$$x^2 - dy^2 = C \tag{2.1}$$

est appelée équation de Pell généralisée. Nous utiliserons indifféremment les notations (x, y) ou $x + y\sqrt{d}$ pour désigner une solution de l'équation (2.1) ; de plus, si x et y sont tous deux strictement positifs, nous dirons que $x + y\sqrt{d}$ est une solution positive de (2.1). Deux solutions $x_1 + y_1\sqrt{d}$ et $x_2 + y_2\sqrt{d}$ sont égales si $x_1 = x_2$ et $y_1 = y_2$.
Pour $C = +1$, on retrouve l'équation classique de Pell :

$$x^2 - dy^2 = 1 \tag{2.2}$$

qui est appelée aussi équation positive de Pell. Pour $C = -1$, on retrouve l'équation

$$x^2 - dy^2 = -1$$

qui est appelée équation négative de Pell. Une équation négative de Pell n'a pas toujours de solution. En effet, considérons l'équation de Pell négative suivante :

$$x^2 - 3y^2 = -1. \tag{2.3}$$

Cette équation n'admet pas de solution. Pour le constater, il suffit de raisonner par l'absurde. Si (2.3) avait une solution (a, b), on aurait $a^2 - 3b^2 = -1$ et $a^2 \equiv -1 \pmod 3$ ou encore $a^2 \equiv 2 \pmod 3$. Or cette congruence est impossible. En suivant la même idée, il est facile de constater que si d est un entier naturel tel que $d \equiv 3 \pmod 4$, alors d n'est pas un carré (car tout carré d'entier est congru à 0 ou à 1 modulo 4) et l'équation de Pell négative

$$x^2 - dy^2 = -1. \tag{2.4}$$

ne possède pas de solution. Pour prouver ce fait, il suffit encore de raisonner par l'absurde. Si l'équation (2.4) avait une solution (a, b), on aurait $a^2 - db^2 = -1$ et $a^2 - db^2 \equiv -1 \pmod 4$ ou encore $a^2 + b^2 \equiv 3 \pmod 4$. Or cette congruence est impossible car comme tout carré d'entier est congru à 0 ou à 1 modulo 4, $a^2 + b^2$ ne peut-être congru qu'à $0, 1$ ou 2 modulo 4 et jamais à 3 modulo 4.

2.3.2 L'équation de Pell positive $x^2 - dy^2 = 1$

Notons que :
- Si $d \leqslant -2$: l'équation $x^2 - dy^2 = 1$ n'admet pas d'autres solutions que $(\pm 1, 0)$.
- Si $d = -1$: l'équation $x^2 - dy^2 = 1$ admet deux solutions que $(\pm 1, 0)$ et $(\pm 0, 1)$.
- Si d est un carré parfait : $x^2 - dy^2 = 1$ devient $(x - y\sqrt{d})(x + y\sqrt{d}) = 1$ cette équation n'admet comme solutions que $(\pm 1, 0)$.

— Si d n'est pas un carré parfait. Pour résoudre $x^2 - dy^2 = 1$ dans $\mathbb{Q}$, il suffit de prendre la relation $(r^2+d)^2 - d(2r)^2 = (r^2-d)^2$ qui est vraie pour tout r et tout d dans $\mathbb{N}$ et de la diviser par $(r^2-d)^2$ pour avoir

$$\left(\frac{(r^2+d)}{(r^2-d)}\right)^2 - d\left(\frac{2r}{r^2-d}\right)^2 = 1,$$

en prenant $x = \frac{(r^2+d)}{(r^2-d)}$ et $y = \frac{2r}{r^2-d}$, on obtient une infinite de solutions dans $\mathbb{Q}$. On montre géométriquement que ce sont les seules solutions.
Trouver les solutions de $x^2 - dy^2 = 1$ dans $\mathbb{Z}$, revient à trouver les éléments α dans $\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \text{ avec } a, b \in \mathbb{Z}\right\}$ tels que $N(\alpha) = 1$, où N désigne l'application norme définie par

$$\begin{array}{rl} N : \mathbb{Z}\left[\sqrt{d}\right] & \longrightarrow \mathbb{Z} \\ \alpha = x + y\sqrt{d} & \longmapsto N(\alpha) = x^2 - dy^2. \end{array}$$

Les éléments α de l'anneau $\mathbb{Z}\left[\sqrt{d}\right]$ avec $N(\alpha) = \pm 1$ sont les unités (les inversibles) de l'anneau $\mathbb{Z}\left[\sqrt{d}\right]$.

Les preuves des théorèmes et propositions suivants reprennent et détaillent celles données dans [40].

Proposition 2.5. *Si $x_1 + y_1\sqrt{d}$ et $x_2 + y_2\sqrt{d}$ sont deux solutions positives de l'équation*

$$x^2 - dy^2 = 1, \tag{2.5}$$

alors les assertions suivantes sont équivalentes :

1. $x_1 < x_2$.
2. $y_1 < y_2$.
3. $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$.

Démonstration. $1 \Longleftrightarrow 2$. On a

$$\begin{array}{rl} x_1 < x_2 & \Longleftrightarrow \; x_1^2 < x_2^2 \Longleftrightarrow x_1^2 - 1 < x_2^2 - 1 \\ & \Longleftrightarrow \; y_1^2 < y_2^2 \Longleftrightarrow y_1 < y_2. \end{array}$$

$1 \Longleftrightarrow 3$. Supposons que $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$. Comme $x_1 + y_1\sqrt{d}$ et $x_2 + y_2\sqrt{d}$ sont solutions de l'équation (2.5), on a $x_1^2 - dy_1^2 = 1$ et $x_2^2 - dy_2^2 = 1$. On en déduit que

$$x_1^2 - dy_1^2 = x_2^2 - dy_2^2.$$

Donc

$$(x_2 - x_1)(x_1 + x_2) = d(y_1 + y_2)(y_2 - y_1).$$

D'une part, cette dernière égalité implique que $(x_2 - x_1)$ et $(y_2 - y_1)$ sont de même signe (car $(x_1 + x_2)$ et $d(y_1 + y_2)$ sont positifs vu que x_1, x_2, y_1, y_2 sont tous positifs). D'autre part, l'hypothèse $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$ donne $(x_2 - x_1) + (y_2 - y_1)\sqrt{d} > 0$. Donc nécessairement $(x_2 - x_1) > 0$ et $(y_2 - y_1) > 0$. D'où $x_1 < x_2$ et $y_1 < y_2$. Réciproquement, il est clair que

$$x_1 < x_2 \Rightarrow y_1 < y_2 \Rightarrow x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}.$$

□

Théorème 2.6. *Soient d un entier positif qui n'est pas un carré parfait et S l'ensemble des solutions positives de l'équation $x^2 - dy^2 = 1$; si $S \neq \emptyset$, alors*

1. *S est infini, ordonné et dénombrable.*
2. *S possède un plus petit élément $\alpha = x_1 + y_1\sqrt{d}$ avec $\alpha > 1$.*

Démonstration. 1. Si $x + y\sqrt{d}$ est une solution non triviale de l'équation $x^2 - dy^2 = 1$, alors on a $(x^2 - dy^2)^2 = 1$, c'est à dire

$$x^4 + d^2y^4 - 2dx^2y^2 = 1.$$

On en déduit que

$$(x^2 + dy^2)^2 - d(2xy)^2 = 1.$$

ainsi $(x^2 + dy^2 + 2xy\sqrt{d})$ est aussi une solution de $x^2 - dy^2 = 1$, strictement supérieure à $x + y\sqrt{d}$. On construit ainsi une suite de solutions strictement croissante. Par conséquent l'équation $x^2 - dy^2 = 1$ possède une infinité de solutions. $S \subset \mathbb{N}\times\mathbb{N}$, $\mathbb{N}\times\mathbb{N}$ étant dénombrable, donc S l'est aussi.

2. D'aprés la proposition 2.5, on peut ordonner les éléments de S suivant l'ordre croissant des x, ou selon l'ordre croissant des y, ou encore selon l'ordre croissant des $x + y\sqrt{d}$, puisque c'est le même ordre. S possède donc un plus petit élément $\alpha = x_1 + y_1\sqrt{d}$ pour lequel les entiers x_1 et y_1 ont leurs plus petites valeurs positives. Comme $\sqrt{d} > 1$ et $x_1 > 0$, $y_1 > 0$ alors $\alpha > 1$.

□

Définition 2.7. *La solution $x + y\sqrt{d}$ de $x^2 - dy^2 = \pm 1$, pour laquelle les entiers x et y ont leurs plus petites valeurs positives, est appelée la solution fondamentale.*

Théorème 2.8. *Soit l'équation de Pell $x^2 - dy^2 = 1$. L'ensemble des solutions avec $x > 0$ et $y > 0$ est*

$$T = \{x_n + y_n\sqrt{d}, n \in \mathbb{N}^*\} = \left\{\left(x_1 + y_1\sqrt{d}\right)^n, n \in \mathbb{N}^*\right\}$$

où $\alpha = (x_1 + y_1\sqrt{d})$ est la solution fondamentale de l'équation. De plus, les suites x_n et y_n vérifient les relations de récurrence suivantes

1. *$x_{n+1} = x_1x_n + dy_1y_n$ et $y_{n+1} = y_1x_n + x_1y_n$.*
2. *$x_{n+1} = 2x_1x_n - x_{n-1}$ et $y_{n+1} = 2x_1y_n - y_{n-1}$.*
3. *$x_n = \frac{\alpha^n + \overline{\alpha}^n}{2}$ et $y_n = \frac{\alpha^n - \overline{\alpha}^n}{2\sqrt{d}}$.*

Démonstration. Par définition de T

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n. \tag{2.6}$$

Comme le conjugué d'un produit est le produit des conjugués, on a

$$x_n - y_n\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)^n. \tag{2.7}$$

En multipliant membre à membre (2.6) et (2.7), on obtient

$$x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n = 1.$$

Ainsi tout élément de T est solution de l'équation $x^2 - dy^2 = 1$, et par suite on a l'inclusion $T \subset S$. Supposons que T soit strictement inclus dans S, alors il existe un élément $(u + v\sqrt{d}) \in S$ et $(u + v\sqrt{d}) \notin T$. Comme les éléments de T constituent une suite strictement croissante, il existe n_0 $\in \mathbb{N}^*$ tel que

$$\left(x_1 + y_1\sqrt{d}\right)^{n_0} < (u + v\sqrt{d}) < \left(x_1 + y_1\sqrt{d}\right)^{n_0+1}.$$

En multipliant par $\left(x_1 - y_1\sqrt{d}\right)^{n_0}$ on obtient

$$1 < (u + v\sqrt{d})\left(x_1 - y_1\sqrt{d}\right)^{n_0} < \left(x_1 + y_1\sqrt{d}\right)$$

$$1 < (x_{n_0} - y_{n_0}\sqrt{d})(u + v\sqrt{d}) < \left(x_1 + y_1\sqrt{d}\right).$$

En posant

$$(x_{n_0} - y_{n_0}\sqrt{d})(u + v\sqrt{d}) = (ux_{n_0} - y_{n_0}vd) + (x_{n_0}v - y_{n_0}u)\sqrt{d} = x^* + y^*\sqrt{d}, \tag{2.8}$$

on obtient

$$(x_{n_0} + y_{n_0}\sqrt{d})(u - v\sqrt{d}) = x^* - y^*\sqrt{d} \tag{2.9}$$

et

$$1 < x^* + y^*\sqrt{d} < \left(x_1 + y_1\sqrt{d}\right). \tag{2.10}$$

En faisant le produit des relations (2.8) et (2.9) on obtient

$$1 = (u^2 - dv^2)(x_{n_0}^2 - dy_{n_0}^2) = (x^*)^2 - d(y^*)^2. \tag{2.11}$$

De (2.10) on a

$$0 < x^* - y^*\sqrt{d} = \frac{1}{x^* + y^*\sqrt{d}} < 1. \tag{2.12}$$

En vertu des relations (2.10) et (2.12), $x^* > 0$ et $y^* > 0$.
De ce qui précède $x^* + y^*\sqrt{d}$ est solution de l'équation $x^2 - dy^2 = 1$ avec $x^* > 0$, $y^* > 0$ et $x^* + y^*\sqrt{d} < x_1 + y_1\sqrt{d}$, cette dernière inégalité stricte est en contradiction avec le fait que $x_1 + y_1\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$, par suite $S \subset T$. D'où l'égalité $S = T$.

1.

$$\begin{aligned} x_{n+1} + y_{n+1}\sqrt{d} &= \left(x_1 + y_1\sqrt{d}\right)^{n+1} \\ &= \left(x_1 + y_1\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)^{n} \\ &= \left(x_1 + y_1\sqrt{d}\right)(x_n + y_n\sqrt{d}) \\ &= (x_1x_n + dy_1y_n) + (y_1x_n + x_1y_n)\sqrt{d}. \end{aligned}$$

D'où

$$\begin{cases} x_{n+1} = x_1x_n + dy_1y_n \\ y_{n+1} = y_1x_n + x_1y_n \end{cases}$$

2. D'une part, on a

$$\begin{cases} x_{n+1} = x_1x_n + dy_1y_n = 2x_1x_n - (x_1x_n - dy_1y_n) \\ y_{n+1} = y_1x_n + x_1y_n = 2y_1y_n - (y_1x_n - x_1y_n) \end{cases}$$

D'autre part

$$\begin{aligned} x_{n-1}+y_{n-1}\sqrt{d} &= \left(x_1+y_1\sqrt{d}\right)^{n-1} \\ &= \left(x_1+y_1\sqrt{d}\right)^{n}\left(x_1+y_1\sqrt{d}\right)^{-1} \\ &= (x_n+y_n\sqrt{d})(x_1-y_1\sqrt{d}) \\ &= (x_1x_n-dy_1y_n)+(-y_1x_n+x_1y_n)\sqrt{d}. \end{aligned}$$

Il en résulte

$$\begin{cases} x_{n+1}=2x_1x_n-x_{n-1} \\ y_{n+1}=2y_1x_n-y_{n-1} \end{cases}$$

3. Si on pose

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}.$$

Alors

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{n-1} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}. \tag{2.13}$$

La matrice $\begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}$ admet les deux valeurs propres $\alpha_1 = x_1+y_1\sqrt{d} = \alpha$ et $\alpha_2 = x_1 - y_1\sqrt{d} = \overline{\alpha}$ et les deux vecteurs propres correspondants sont $V_\alpha = \begin{pmatrix} 1 \\ \frac{1}{\sqrt{d}} \end{pmatrix}$ et $V_{\overline{\alpha}} = \begin{pmatrix} -\sqrt{d} \\ 1 \end{pmatrix}$. Si on note par P la matrice de passage, alors $P = \begin{pmatrix} 1 & -\sqrt{d} \\ \frac{1}{\sqrt{d}} & 1 \end{pmatrix}$, d'où

$$\begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{n-1} = P\begin{pmatrix} \alpha^{n-1} & 0 \\ 0 & \overline{\alpha}^{n-1} \end{pmatrix}P^{-1} = \begin{pmatrix} \frac{\alpha^{n-1}+\overline{\alpha}^{n-1}}{2} & \frac{\sqrt{d}(\alpha^{n-1}-\overline{\alpha}^{n-1})}{2} \\ \frac{\alpha^{n-1}-\overline{\alpha}^{n-1}}{2\sqrt{d}} & \frac{\alpha^{n-1}+\overline{\alpha}^{n-1}}{2} \end{pmatrix}.$$

La relation (2.13) donne

$$\begin{cases} x_n = \frac{\alpha^n+\bar{\alpha}^n}{2}, \\ y_n = \frac{\alpha^n-\bar{\alpha}^n}{2\sqrt{d}}. \end{cases}$$

□

2.3.3 L'équation de Pell négative $x^2 - dy^2 = -1$

Trouver les solutions de l'équation $x^2 - dy^2 = -1$ dans $\mathbb{Z}$, revient à trouver les éléments α dans $\mathbb{Z}\left[\sqrt{d}\right]$ tels que $N(\alpha) = -1$, où N désigne l'application norme. L'équation $x^2 - dy^2 = -1$ peut ne pas avoir de solutions mais si elle en a une, elle en a une infinité.

Le théorème suivant donne deux conditions nécessaires pour que l'équation de Pell négative admette des solutions.

Proposition 2.9 ([40]). *Supposons que l'équation $x^2 - dy^2 = -1$ possède des solutions, alors*

1. *Si d est pair, alors d est de la forme $4k+2$, où $k \in \mathbb{N}$.*
2. *Tout diviseur premier impair de d est de la forme $4k+1$, où $k \in \mathbb{N}$.*

Le théorème suivant donne explicitement l'ensemble des solutions en entiers positifs de l'équation $x^2 - dy^2 = \pm 1$.

Théorème 2.10 ([40]). *Si l'équation $x^2 - dy^2 = -1$ possède des solutions et $x_1 + y_1\sqrt{d}$ est sa solution fondamentale, alors*

1. *$(x_1 + y_1\sqrt{d})^2$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$.*
2. *L'ensemble des solutions en entiers positifs de l'équation $x^2 - dy^2 = 1$ est*

$$S_2 = \left\{(x_1 + y_1\sqrt{d})^{2k}, k \in \mathbb{N}\right\}.$$

3. *L'ensemble des solutions en entiers positifs de l'équation $x^2 - dy^2 = -1$ est*

$$S_1 = \left\{(x_1 + y_1\sqrt{d})^{2k+1}, k \in \mathbb{N}\right\}.$$

Exemple 2.11. *L'équation $x^2 - 34y^2 = -1$ ne possède aucune solution malgré que les deux conditions nécessaires sont satisfaites. En effet. Si l'équation $x^2 - 34y^2 = -1$ possédait des solutions et $x_1 + y_1\sqrt{d}$ est sa solution fondamentale, alors $(x_1 + y_1\sqrt{d})^2$ serait la solution fondamentale de l'équation $x^2 - 34y^2 = +1$. Or cette dernière a pour solution fondamentale $35 + 6\sqrt{34}$, ce qui donne le système d'équations suivant*

$$\begin{cases} x_1^2 + dy_1^2 = 35, \\ 2x_1y_1 = 6, \end{cases}$$

mais ce dernier système d'équations ne possède pas de solutions dans $\mathbb{N}$. Donc l'équation $x^2 - 34y^2 = -1$ n'admet pas de solutions.

L'équation $x^2 - 5y^2 = -1$ admet $2 + \sqrt{5}$ comme solution fondamentale, les solutions entières positives sont $\left\{(2 + \sqrt{5})^{2k+1}, k \in \mathbb{N}\right\}$.

L'équation $x^2 - 5y^2 = +1$ admet comme solution fondamentale $(2 + \sqrt{5})^2 = 9 + 4\sqrt{5}$, les solutions entières positives sont $\left\{(2 + \sqrt{5})^{2k}, k \in \mathbb{N}\right\}$.

Théorème 2.12. *Soit p un nombre premier impair, l'équation $x^2 - py^2 = -1$ admet des solutions si et seulement si p est de la forme $4k + 1$.*

Démonstration. Notons d'abord que : Si $p = 2$, l'équation $x^2 - 2y^2 = -1$ admet des solutions et $1 + \sqrt{2}$ est sa solution fondamentale.

Si $p > 2$ et l'équation $x^2 - py^2 = -1$ admet une solution $x_0 + y_0\sqrt{d}$, alors $x_0^2 + 1 = py_0^2$ donc p divise $x_0^2 + 1$, autrement dit, $x_0^2 \equiv -1 \pmod{p}$ c'est a dire $\left(\frac{-1}{p}\right) = 1$. Donc $p = 4k + 1$ pour un certain $k \in \mathbb{N}^*$.

Réciproquement, supposons que $p = 4k + 1$, $k \in \mathbb{N}^*$. Si $x_0 + y_0\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - py^2 = +1$, nécessairement x_0 est impair (sinon x_0 est pair entraine $y_0^2 \equiv 3 \pmod{4}$, ce qui est impossible). L'égalité

$$x_0^2 - 1 = (x_0 - 1)(x_0 + 1) = py_0^2$$

montre que $\text{pgcd}(x_0 - 1, x_0 + 1) = 2$. On a donc deux possibilités :

Cas 1 : $x_0 - 1 = 2pt^2$ et $x_0 + 1 = 2s^2$, avec $y_0 = 2st$ et s et t sont dans $\mathbb{N}^*$. Ceci implique $s^2 - dt^2 = 1$ avec $t < y_0$, ce qui est imposible car $x_0 + y_0\sqrt{d}$ est la solution fondamentale de $x^2 - py^2 = +1$.

Cas 2 : $x_0 - 1 = 2s^2$ et $x_0 + 1 = 2pt^2$ avec $s^2 - pt^2 = -1$ autrement dit $s + t\sqrt{d}$ est une solution de l'équation $x^2 - py^2 = -1$. $y_0 = 2st$ et $x_0 = s^2 + pt^2$ donc $x_0 + y_0\sqrt{d} = (s + t\sqrt{d})^2$. Ainsi la solution $s + t\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - py^2 = -1$ en vertu du théorème 2.10. □

En 2010, R. A. Mollin et A. Srinivasan ont donné un critère simple pour vérifier si l'équation $x^2 - dy^2 = -1$ admet des solutions ou non, connaissant la solution fondamentale de l'équation $x^2 - dy^2 = 1$, mais le problème revient à la recherche de la solution fondamentale de l'équation $x^2 - dy^2 = 1$.

Théorème 2.13 ([38]). *L'équation*

$$x^2 - dy^2 = -1 \tag{2.14}$$

où $d \equiv 1 \pmod 4$ *ou* $d \equiv 2 \pmod 4$, *possède des solutions si et seulement si* $x_0 \equiv -1 \pmod{2d}$ *où* $(x_0 + y_0\sqrt{d}\ )$ *est la solution fondamentale de l'équation* $x^2 - dy^2 = +1$.

Remarque 2.14. *Les cas* $d \equiv 0 \pmod 4$ *et* $d \equiv 3 \pmod 4$ *ont été exclus du théorème précédent car si* $d \equiv 0 \pmod 4$, *l'équation* $x^2 - dy^2 = 1$ *ne possède pas de solutions en vertu de la proposition 2.9. Si* $d \equiv 3 \pmod 4$, *l'équation* $x^2 - dy^2 = 1$ *ne possède pas non plus de solutions en vertu de la proposition 2.9.*

Démonstration. Supposons que l'équation $x^2 - dy^2 = -1$ admet des solutions,et notons sa solution fondamentale par $x_1 + y_1\sqrt{d}$, alors $(x_1 + y_1\sqrt{d})^2 = x_0 + y_0\sqrt{d}$ est la solution fondamentale de $x^2 - dy^2 = +1$. D'où $x_0 = x_1^2 + y_1^2 d$ et $y_0 = 2x_1y_1$. Par suite on a

$$x_0 = -1 + 2y_1^2 d \equiv -1 \pmod{2d}.$$

Réciproquement : supposons que la solution fondamentale $x_0 + y_0\sqrt{d}$ de l'équation $x^2 - dy^2 = +1$ vérifie $x_0 \equiv -1 \pmod{2d}$. Donc $x_0 = 2dk - 1$, $k \in \mathbb{N}^*$. En l'injectant dans l'équation $x^2 - dy^2 = +1$, on obtient $(2dk-1)^2 - dy_0^2 = 1$. Autrement dit $4k(dk-1) = y_0^2$. Alors nécessairement y_0 est pair. Posons $y_0 = 2y_*$. On obtient $k(dk-1) = y_*^2$. Comme k et $(kd-1)$ sont premiers entre eux et leur produit est un carré, nécessairement eux-mêmes sont aussi des carrés. Donc $k = m^2$ pour un certain $m \in \mathbb{N}^*$ et $(kd-1) = n^2$ pour un certain $n \in \mathbb{N}^*$. Par suite, $m^2 d - 1 = n^2$. D'où $n^2 - dm^2 = -1$, autrement dit $n + m\sqrt{d}$ est solution de l'équation $x^2 - dy^2 = -1$. □

2.3.4 Période de $\sqrt{d}$ et solution fondamentale de l'équation de Pell $x^2 - dy^2 = \pm 1$

Soit $\alpha = x_1 + y_1\sqrt{d}$ la solution fondamentale de l'équation de Pell $x^2 - dy^2 = +1$ et $x_n + y_n\sqrt{d} = \alpha^n$, alors

$$x_n - y_n\sqrt{d} = \frac{1}{x_n + y_n\sqrt{d}}$$

Par suite

$$\frac{x_n}{y_n} - \sqrt{d} = \frac{1}{y_n(x_n + y_n\sqrt{d})} < \frac{1}{2y_n^2}.$$

Comme $\alpha > 1$, la suite $(\alpha^n)_{n\geqslant 0}$ est strictement croissante, alors la suite y_n tend vers l'infini. Par suite, $\frac{x_n}{y_n}$ est une bonne approximation rationnelle de $\sqrt{d}$ avec une erreur inférieure à $\frac{1}{2y_n^2}$. Par conséquent c'est une réduite de $\sqrt{d}$. Le développement en fraction continue de $\sqrt{d}$ permet de dire si l'équation $x^2 - dy^2 = -1$ possède des solutions ou non ; ce développement nous fournit la solution fondamentale en termes de réduites et il permet aussi d'approcher $\sqrt{d}$ comme le montre le théorème suivant :

Théorème 2.15 ([56]). *Soit* ℓ *la période du développement en fraction continue de*

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

- *Si* ℓ *est pair, la solution fondamentale de l'équation* $x^2 - dy^2 = 1$ *est* $p_{\ell-1} + q_{\ell-1}\sqrt{d}$ *où* $\dfrac{p_{\ell-1}}{q_{\ell-1}} = [a_0, a_1, a_2, \ldots, a_{\ell-1}]$. *Mais l'équation* $x^2 - dy^2 = -1$ *ne possède pas de solution.*
- *Si* ℓ *est impair, la solution fondamentale de l'équation* $x^2 - dy^2 = -1$ *est* $p_{\ell-1} + q_{\ell-1}\sqrt{d}$ *où* $\dfrac{p_\ell}{q_\ell} = [a_0, a_1, a_2, \ldots, a_{\ell-1}]$ *et la solution fondamentale de l'équation* $x^2 - dy^2 = 1$ *est*

$(p_{\ell-1} + q_{\ell-1}\sqrt{d})^2$.

Exemple 2.16. *1.* $x^2 - 2y^2 = \pm 1$.

$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1}$. *Par suite* $\sqrt{2} = \left[1, \overline{2}\right]$, *la période* $\ell = 1$, *étant impaire, l'équation* $x^2 - 2y^2 = -1$ *admet des solutions,* $\frac{p_0}{q_0} = [a_0] = \frac{1}{1}$ *; sa solution fondamentale est* $1 + 1\sqrt{2}$. *La solution fondamentale de l'équation* $x^2 - 2y^2 = +1$ *est* $(1 + 1\sqrt{2})^2 = 3 + 2\sqrt{2}$.

2. $x^2 - 3y^2 = \pm 1$.

$\sqrt{3} = \left[1, \overline{1, 2}\right]$, la période étant $\ell = 2$ pair, $\frac{p_1}{q_1} = [a_0, a_1] = \frac{2}{1}$, la solution fondamentale de l'équation $x^2 - 3y^2 = 1$ est $2 + 1\sqrt{3}$, mais l'équation $x^2 - 3y^2 = -1$ n'admet pas de solutions.

Les algorithmes les plus pratiques, et les plus efficaces, utilisés pour le calcul de la solution fondamentale sont :

- L'Algorithme LMM (Lagrange-Mathew -Molin) : cet algorithme était déjà connu par Lagrange (voir [38] et [37]) .
- L'Algorithme de Lenstra (voir [26] et [27]).
- L'Algorithme de Lagarias : cet algorithme suppose la confirmation de l'hypothèse de Riemann [25].

2.3.5 L'équation de Pell $x^2 - dy^2 = C$

Notons d'abord que :

- L'équation $ax^2 + bxy + cy^2 = C$, où a, b, c et C sont dans $\mathbb{Z}$, peut être ramenée à l'équation $X^2 - DY^2 = C'$ via les changements de variables $X = 2ax + by$, $Y = y$, $D = b^2 - 4ac$ et $C' = 4aC$.
- Trouver les solutions de l'équation $x^2 - dy^2 = C$, dans $\mathbb{Z}$, revient à trouver les éléments α dans $\mathbb{Z}\left[\sqrt{d}\right]$ tels que $N(\alpha) = C$, où N désigne l'application norme.
- Cette équation peut aussi ne pas avoir de solutions mais si elle en a une, elle en a une infinité. Ainsi l'équation $x^2 - 5y^2 = 2$, n'admet pas de solution car l'équation $x^2 \equiv 2 \pmod 5$ n'admet pas de solution.

La proposition suivante va nous permettre de relier les solutions de l'équation $x^2 - dy^2 = C$, $C \neq 1$ et celles de l'équation $x^2 - dy^2 = 1$.

Proposition 2.17. *Si* $(u + v\sqrt{d})$ *est solution de l'équation* $x^2 - dy^2 = C$ *et* $(x + y\sqrt{d})$ *est solution de l'équation* $x^2 - dy^2 = 1$, *alors* $(x + y\sqrt{d})(u + v\sqrt{d}) = (xu + yvd) + (xv + yu)\sqrt{d}$ *est solution de l'équation* $x^2 - dy^2 = C$.

Démonstration. le résultat découle directement de la relation $(ux + vyd)^2 - d(yu + vx)^2 = (u^2 - dv^2)(x^2 - dy^2)$, ou encore grâce à la propriété de la norme suivante $N((x + y\sqrt{d})(u + v\sqrt{d})) = N(x + y\sqrt{d})N(u + v\sqrt{d})$. □

En 1909, le mathématicien Norvégien Axel Thue [51] a démontré un théorème important dont une des conséquences directes est que si $f(z) = a_n z^n + \ldots + a_1 z + a_0 \in \mathbb{Z}[X]$, deg $f \geqslant 3$ et f irréductible, alors l'équation diophantienne

$$y^n f\left(\frac{x}{y}\right) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_0 y^n = C,$$

où $C \in \mathbb{Z}^*$, soit ne possède pas de solutions du tout, ou bien elle en a un nombre fini. Comme pour l'équation de Pell on a $n = 2$, on ne peut donc pas appliquer le résultat de Thue.

Sur l'ensemble des solutions de l'équation $x^2 - dy^2 = C$, on définit une relation d'équivalence comme suit :

$$(u_1 + v_1\sqrt{d}) \sim (u_2 + v_2\sqrt{d})$$

s'il existe $(x+y\sqrt{d})$ solution de l'équation $x^2-dy^2=1$ telle que $(u_2+v_2\sqrt{d}) = (u_1+v_1\sqrt{d})(x+y\sqrt{d})$. Deux solutions $(u_1 + v_1\sqrt{d})$ et $(u_2 + v_2\sqrt{d})$ de l'équation $x^2 - dy^2 = C$ sont dites associées si elles sont dans la même classe d'équivalence de solutions.

Proposition 2.18. *Deux solutions $(u_1 + v_1\sqrt{d})$ et $(u_2 + v_2\sqrt{d})$ de l'équation $x^2 - dy^2 = C$ sont associées si et seulement si $u_1u_2 - v_1v_2d$ et $u_2v_1 - u_1v_2$ sont des multiples de C.*

Démonstration. Supposons $(u_1 + v_1\sqrt{d})$ et $(u_2 + v_2\sqrt{d})$ deux solutions associées de l'équation $x^2 - dy^2 = C$, donc il existe $u+v\sqrt{d}$ solution de $x^2-dy^2=1$ tels que $(u_2+v_2\sqrt{d}) = (u_1+v_1\sqrt{d})(u+v\sqrt{d})$. Ceci donne

$$\begin{cases} u_2 = uu_1 + dvv_1 \\ v_2 = uv_1 + vu_1 \end{cases}$$

Ce qui donne

$$\begin{cases} u_2u_1 = uu_1^2 + dvv_1u_1 \\ dv_2v_1 = duv_1^2 + dvu_1v_1 \end{cases} \tag{2.15}$$

En soustrayant la première équation de la seconde dans le système (2.15), on obtient $u_2u_1 - dv_2v_1 = uC$. De la même manière, nous obtenons $v_1u_2 - u_1v_2 = -vC$. D'où $u_2u_1 - dv_2v_1$ et $v_1u_2 - u_1v_2$ sont multiples de C.
Réciproquement, supposons $\left(u_1 + v_1\sqrt{d}\right)$ et $\left(u_2 + v_2\sqrt{d}\right)$ sont solutions de l'équation $x^2-dy^2 = C$, tels que $u_2u_1 - dv_2v_1 = uC$ et $v_1u_2 - u_1v_2 = vC$ pour certains u et v dans $\mathbb{Z}$, alors

$$u = \frac{u_2u_1 - dv_2v_1}{C}, \quad v = \frac{v_1u_2 - u_1v_2}{C}$$

et $\left(u + v\sqrt{d}\right)$ est une solution de $x^2 - dy^2 = 1$ de plus

$$\left(u_1 + v_1\sqrt{d}\right) = \left(u + v\sqrt{d}\right)\left(u_2 + v_2\sqrt{d}\right),$$

d'où les solutions $\left(u_1 + v_1\sqrt{d}\right)$ et $\left(u_2 + v_2\sqrt{d}\right)$ sont associées. □

Définition 2.19. *Si K est une classe de solutions de l'équation $x^2 - dy^2 = C$, l'ensemble $\overline{K} = \{(u - v\sqrt{d})/(u + v\sqrt{d}) \in K\}$ est aussi une classe de solutions de la même équation et dite classe conjuguée de la classe K de solutions et notée $\overline{K}$.*

Si $K = \overline{K}$, on dit que la classe est ambigue. Dans une classe K de solutions non ambigue, il existe une seule solution $u^* + v^*\sqrt{d}$ avec v^* positif minimal ($(-u^* + v^*\sqrt{d}) = -(u^* - v^*\sqrt{d})$ étant dans $\overline{K}$), cette solution est dite solution fondamentale de la classe K de solutions. De même dans une classe ambigue K, il existe une seule solution $u^* + v^*\sqrt{d}$ avec v^* positif minimal et $u^* \geqslant 0$, cette solution est dite solution fondamentale de la classe K.

Remarque 2.20. *Si K est une classe de solutions non ambigue et $u^* + v^*\sqrt{d}$ est sa solution fondamentale, alors $-u^* + v^*\sqrt{d}$ est la solution fondamentale de la classe conjuguée de solutions $\overline{K}$.*

Exemple 2.21. $x^2 - 7y^2 = 9$
On a au moins trois classes de slutions : la classe de $(3 + 0\sqrt{7})$, la classe de $(4 + 1\sqrt{7})$ et la classe de $(-4 + 1\sqrt{7})$.

Si $u + v\sqrt{d}$ est une solution positive de l'équation $x^2 - dy^2 = -C$, alors $u + v\sqrt{d}$ est dans une certaine classe de solutions K, et il existe $m \in \mathbb{N}$ tel que $\left(u + v\sqrt{d}\right) = \left(u^* + v^*\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)^m$

où $\left(x_1 + y_1\sqrt{d}\right)$ est la solution fondamentale de $x^2 - dy^2 = 1$ et $\left(u^* + v^*\sqrt{d}\right)$ est la solution fondamentale de la classe K. Si $u + v\sqrt{d}$ est une solution positive de l'équation $x^2 - dy^2 = C$, alors $u + v\sqrt{d}$ est dans une certaine classe de solutions K, et il existe $m \in \mathbb{N}$ tels que

$$\left(u + v\sqrt{d}\right) = \left(u^* + v^*\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right)^m$$

où $\left(x_1 + y_1\sqrt{d}\right)$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$ et $\left(u^* + v^*\sqrt{d}\right)$ est la solution fondamentale de la classe K.

Les deux lemmes suivants, dûs à Nagell [40], sont fondamentaux dans l'étude des équations de Pell ; ils nous seront utiles pour les preuves des théorèmes 2.41 et 2.42.

Lemme 2.22. *Si $u + v\sqrt{d}$ est la solution fondamentale d'une classe K de solutions de l'équation $x^2 - dy^2 = C$ et $x_1 + y_1\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$, alors*

$$0 <\mid u \mid\leqslant \sqrt{\frac{(x_1+1)C}{2}} \quad \text{et} \quad 0 \leqslant v \leqslant y_1\sqrt{\frac{C}{2(x_1+1)}}.$$

Démonstration. La remarque 2.20 montre que si les inégalités sont vraies pour une classe K, elles le sont pour la classe conjuguée $\overline{K}$, on peut donc supposer $u > 0$.
Comme $x_1+y_1\sqrt{d}$ (respectivement $(u+v\sqrt{d})$) est solution de l'équation $x^2-dy^2 = 1$ (respectivement est solution de $u^2 - dv^2 = C$), on a

$$x_1^2 - dy_1^2 = 1 \quad \text{et} \quad u^2 - dv^2 = C.$$

Par suite

$$d^2v^2y_1^2 = (x_1^2 - 1)(u^2 - C)$$

d'où

$$dv_1y_1 = \sqrt{(x_1^2 - 1)(u^2 - C)}$$

$$ux_1 - dvy_1 = ux_1 - \sqrt{(x_1^2 - 1)(u^2 - C)}$$

Comme $(u+v\sqrt{d})(x_1-y_1\sqrt{d}) = (ux_1-dvy_1)+(x_1v-y_1u\,)\sqrt{d}$ est une solution associée à la solution $(u + v\sqrt{d})$, elle est dans la même classe que $(u + v\sqrt{d})$; or $(u + v\sqrt{d})$ est la solution fondamentale d'où $u \leqslant ux_1 - dvy_1$. Par suite $dvy_1 \leqslant u(x_1 - 1)$. D'où

$$d^2v^2y_1^2 = (x_1^2 - 1)(u^2 - C) \leqslant u^2(x_1 - 1)^2,$$

et

$$\left(1 - \frac{C}{u^2}\right)(x_1 + 1) \leqslant (x_1 - 1).$$

Par suite

$$u^2 \leqslant C\frac{(x_1 + 1)}{2}. \tag{2.16}$$

Par conséquent

$$0 <\mid u \mid\leqslant \sqrt{\frac{(x_1 + 1)C}{2}}.$$

Pour obtenir la deuxième inégalité, il suffit de voir que de (2.16) on a

$$0 < dv^2 + C \leqslant C\frac{(x_1 + 1)}{2}.$$

Donc

$$0 < dv^2 \leqslant \frac{(x_1-1)}{2}C.$$

Ainsi on a

$$0 < v^2 \leqslant \frac{y_1^2 C}{2(x_1+1)}.$$

D'où

$$0 \leqslant v \leqslant \frac{y_1}{\sqrt{2(x_1+1)}}\sqrt{C}.$$

□

Exemple 2.23. $x^2 - 7y^2 = 9$
La solution fondamentale de l'équation $x^2 - 7y^2 = +1$ *étant* $8 + 3\sqrt{7}$. *On cherche les solutions* $u + v\sqrt{d}$ *avec* $0 <\mid u \mid\leqslant \sqrt{\frac{(8+1)9}{2}}$,*(d'après le lemme précédent), d'où l'équation* $x^2 - 7y^2 = 9$ *possède exactement trois classes de solutions : la classe de* $(3 + 0\sqrt{7})$, *la classe de* $(4 + 1\sqrt{7})$ *et la classe de* $(-4 + 1\sqrt{7})$.

Lemme 2.24. *Si* $u + v\sqrt{d}$ *est la solution fondamentale d'une classe de solutions* K *de l'équation* $x^2 - dy^2 = -C$ *et* $x_1 + y_1\sqrt{d}$ *est la solution fondamentale de l'équation* $x^2 - dy^2 = 1$, *alors*

$$0 < v \leqslant \frac{y_1}{\sqrt{2(x_1-1)}}\sqrt{C} \quad \text{et} \quad 0 \leqslant\mid u \mid\leqslant \sqrt{\frac{(x_1-1)C}{2}}.$$

Démonstration. La remarque 2.20 montre encore que si les inégalités précédentes sont vraies pour une classe K, alors elles le sont aussi pour la classe conjuguée $\overline{K}$, on peut donc supposer $u > 0$.

$$(u + v\sqrt{d})(x_1 - y_1\sqrt{d}) = (ux_1 - dvy_1) + (x_1v - y_1u)\sqrt{d}$$

est une solution de l'équation $u^2 - dv^2 = -C$, associée à la solution $(u + v\sqrt{d})$, elle est donc dans la même classe K que $(u + v\sqrt{d})$; or $(u + v\sqrt{d})$ est la solution fondamentale, on aura nécessairement

$$v \leqslant (x_1v - y_1u).$$

D'où

$$y_1u \leqslant v(x_1 - 1).$$

Par suite

$$dy_1^2u^2 \leqslant dv^2(x_1 - 1)^2.$$

En remplaçant u^2 par $-C + dv^2$ on obtient

$$dy_1^2(dv^2 - C) \leqslant dv^2(x_1 - 1)^2.$$

Autrement dit

$$(dv^2 - C)\frac{x_1+1}{x_1-1} \leqslant dv^2.$$

Il en résulte que

$$\frac{x_1+1}{x_1-1} \leqslant 1 + \frac{C}{(dv^2 - C)}.$$

En remplaçant dans cette dernière inégalité $(dv^2 - C)$ par u^2, on obtient

$$u^2 \leqslant \frac{C(x_1 - 1)}{2}. \tag{2.17}$$

D'où

$$0 \leqslant \mid u \mid \leqslant \sqrt{\frac{(x_1 - 1)C}{2}}.$$

De la relation $u^2 - dv^2 = -C$ on tire

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

On l'injecte dans l'inégalité (2.17) on obtient :

$$dv^2 \leqslant C\frac{(x_1 + 1)}{2}.$$

Ainsi on a

$$v^2 \leqslant C\frac{y_1^2}{2(x_1 - 1)}.$$

D'où l'inégalité

$$0 < v \leqslant \frac{y_1}{\sqrt{2(x_1 - 1)}}\sqrt{C}.$$

□

Des deux lemmes precédents, on peut conclure que :

— Les solutions fondamentales sont à rechercher entre les bornes fournies par ces deux lemmes ; donc si l'équation ne possède pas de solutions entre ces bornes, c'est qu'elle ne possède pas de solutions du tout.

— Les bornes étant finies et les solutions cherchées étant des entiers, alors le nombre de classes de solutions est fini.

Exemple 2.25. *$x^2 - 5y^2 = \pm 4$. La solution fondamentale de l'équation $x^2 - 5y^2 = +1$ étant $9 + 4\sqrt{5}$, alors l'équation $x^2 - 5y^2 = 4$ possède trois classes de solutions K_1, K_2 et K_3 avec $2 + 0\sqrt{5}$ solution fondamentale de K_1, $3 + \sqrt{5}$ solution fondamentale de K_2, $-3 + \sqrt{5}$ solution fondamentale de K_3. L'équation $x^2 - 5y^2 = -4$ possède trois classes de solutions $K_1^{'}$, $K_2^{'}$ et $K_3^{'}$ avec $1 + \sqrt{5}$ solution fondamentale de $K_1^{'}$, $-1 + \sqrt{5}$ solution fondamentale de $K_2^{'}$ et $4 + 2\sqrt{5}$ solution fondamentale de $K_3^{'}$ ($K_3^{'}$ est une classe ambigue).*

2.4 Sur l'équation diophantienne $x^2 - kxy + y^2 \pm 2^n = 0$

2.4.1 Introduction

Dans cette section, nous allons nous intéresser à la résolution de certaines équations diophantiennes de la forme

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{2.18}$$

où a, b, c, d, e et f sont des entiers fixés.

Généralement, on veut seulement savoir si cette équation possède des solutions entières positives $(x, y) \in \mathbb{N}^2$ ou simplement des solutions entières $(x, y) \in \mathbb{Z}^2$ ou encore dans certains cas des solutions rationnelles $(x, y) \in \mathbb{Q}^2$. Dans le cas où celà s'avère possible, on souhaite déterminer explicitement l'ensemble des solutions de cette équation.

Nous désignerons par

$$S\left\{ax^2 + bxy + cy^2 + dx + ey + f = 0\right\}$$

l'ensemble des solutions entières positives $(x, y) \in \mathbb{N}^2$ vérifiant (2.18) et par $\#E$ le cardinal d'un ensemble E. Nous désignerons aussi par $S_1\left\{ax^2 + bxy + cy^2 + dx + ey + f = 0\right\}$ l'ensemble des solutions entières impaires positives $(x, y) \in \mathbb{N}^2$ vérifiant (2.18). Autrement dit, en posant $P(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$, $S\{P(x, y) = 0\}$ et $S_1\{P(x, y) = 0\}$ désignent les ensembles suivants :

$$S\{P(x,y) = 0\} = \left\{(x,y) \in \mathbb{N}^2 \ / \ P(x,y) = 0\right\},$$

$$S_1\{P(x,y) = 0\} = \left\{(x,y) \in \mathbb{N}^2 \ / \ P(x,y) = 0 \text{ et } x \equiv 1 \pmod 2 \text{ et } y \equiv 1 \pmod 2\right\}.$$

L'équation diophantienne

$$x^2 - kxy + y^2 + \ell x = 0 \tag{2.19}$$

où k et ℓ sont des entiers a fait l'objet de plusieurs études ces dernières années. Ainsi, en 2004, Marlewski et Zarzycki [31] ont étudié l'équation (2.19) pour $\ell = 1$ et ont prouvé que l'équation (2.19) n'a pas de solution positive pour $\ell = 1$ et $k > 3$, mais possède une infinité de solutions pour $k = 3$ et $\ell = 1$.

En 2013, Y. Hu et M. Le [18] ont donné une condition nécessaire et suffisante sur k pour que l'équation admette une infinité de solutions en la ramenant à une équation de Pell.

Dans [21], Keskin, Siar et Karaatli ont considéré l'équation (2.19) pour $\ell = -1$ et ont prouvé qu'elle possède des solutions entières positives pour $k > 1$. Yuan et Hu [57] ont considéré l'équation (2.19) pour $\ell = 1, 2$ ou 4 et ont déterminé les valeurs de l'entier k, pour lesquelles l'équation (2.19) possède une infinité de solutions entières positives. Poursuivant les travaux de Yuan et Hu [57], Keskin, Siar et Karaatli dans [22] et [23] ont considéré l'équation (2.19) pour $\ell = \pm 2^r$ où r est un entier positif. Ils ont montré comment, pour que l'équation (2.19) avec $\ell = -2^r$ possède une infinité de solutions entières positives, il suffit de déterminer les cas où l'équation diophantienne

$$x^2 - kxy + y^2 - 2^n = 0. \tag{2.20}$$

possède une infinité de solutions entières positives x et y. D'une manière similaire, en posant $\ell = 2^r$ dans l'équation (2.19), nous avons seulement besoin de considérer l'équation diophantienne

$$x^2 - kxy + y^2 + 2^n = 0. \tag{2.21}$$

En 2013, Keskin, Siar et Karaatli ont résolu l'équation (2.20) et l'équation (2.21) pour $0 \leqslant n \leqslant 10$ et à la lumière des résultats obtenus [23] ils ont proposé la conjecture suivante.

Conjecture 2.26. *Soit l'équation diophantienne*

$$x^2 - kxy + y^2 = 2^n. \tag{2.22}$$

1. *Pour n impair et $n \geqslant 3$, on a :*
   - *Si $k > 2^n - 2$, l'équation (2.22) n'admet pas de solution positive,*
   - *Si $k \leqslant 2^n - 2$ et l'équation (2.22) admet une solution, alors k est pair.*
2. *Pour n pair et $n \geqslant 2$, on a :*
   - *Si $k > 2^n - 2$, l'équation (2.22) n'admet pas de solution entière impaire,*
   - *Si $k \leqslant 2^n - 2$ et l'équation (2.22) admet une solution positive impaire, alors k est pair.*

2.4.2 Travaux de Keskin, Siar et Karaatli

Pour établir les nombreux théorèmes contenus dans leurs articles, Keskin, Karaatli et Siar ont exploité non seulement les théorèmes classiques concernant les équations diophantiennes de Pell (que nous avons étudiées dans la première section de ce chapitre), mais aussi de nombreux autres

résultats préalablement établis dans d'autres articles. Dans ce paragraphe, nous n'examinerons que quelques uns d'entre eux.

Le théorème suivant se trouve dans [20], [21], [29], [34] et dans [23, Theorème 3.1].

Théorème 2.27 ([23]). *Soit $k \geqslant 3$. Alors toutes les solutions entières positives de l'équation $x^2 - kxy + y^2 - 1 = 0$ sont données par $(x, y) = (u_n, u_{n-1})$ avec $n > 1$, où $u_n = F_n(k, -1)$.*

Dans [23] , Keskin, Karaatli et Siar déduisent du théorème précédent le corollaire suivant (Corollaire 3.1 dans [23])

Corollaire 2.28 ([23]). *Soit $r \geqslant 1$. Alors toutes les solutions entières positives de l'équation $x^2 - kxy + y^2 - 2^{2r} = 0$ sont données par $(x, y) = (2^r u_n, 2^r u_{n-1})$ avec $n > 1$, où $u_n = F_n(k, -1)$.*

Le théorème suivant est le théorème 3.2, p.792 dans [23].

Théorème 2.29 ([23]). *Soit $r \geqslant 2$ un entier. Alors toutes les solutions entières positives de l'équation $x^2 - \left(2^{2r} - 2\right) xy + y^2 - 2^{2r} = 0$ sont données par $(x, y) = (u_{n+1}, u_{n-1})$ avec $n > 1$, où $u_n = F_n(2^r, -1)$.*

Ce théorème est suivi de quatre corollaires (corollaires 3.2, 3.3, 3.4 et 3.5) correspondant à une application du théorème 3.2 pour $r \in \{1, 2, 3, 4\}$.

Le théorème suivant est le théorème 3.3, p793 de [23]

Théorème 2.30 ([23]). *Soit $r > 1$ un entier impair. Alors toutes les solutions entières positives de l'équation $x^2 - (2^r - 2) xy + y^2 - 2^r = 0$ sont données par $(x, y) = (u_{n+1} + u_n, u_n + u_{n-1})$ avec $n \geqslant 1$, où $u_n = F_n(2^r - 2, -1)$.*

Ce théorème est suivi de quatre corollaires (corollaires 3.6, 3.7, 3.8 et 3.9) correspondant à une application du théorème 3.3 pour $r \in \{3, 5, 7, 9\}$.

Keskin, Siar et Karaatli déterminent ensuite les solutions entières positives des équations

$$\begin{aligned} x^2 - \frac{1}{3}(2^r - 10) xy + y^2 - 2^r &= 0, \\ x^2 - \frac{1}{5}(2^r - 26) xy + y^2 - 2^r &= 0, \\ x^2 - \frac{1}{7}(2^r - 50) xy + y^2 - 2^r &= 0, \\ x^2 - \frac{1}{11}(2^r - 122) xy + y^2 - 2^r &= 0. \end{aligned}$$

et obtiennent les théorèmes suivants (théorèmes 3.4, 3.5, 3.6 et 3.7 de [23]).

Théorème 2.31 ([23]). *Soit $r > 0$ un entier pair. Alors toutes les solutions entières positives de l'équation $x^2 - \frac{1}{3}(2^r - 10) xy + y^2 - 2^r = 0$ sont données par $(x, y) = (u_{n+2} + 3u_{n+1}, u_{n+1} + 3u_n)$ avec $n \geqslant 0$, où $u_n = F_n\left(\frac{1}{3}(2^r - 10), -1\right)$.*

Ce théorème est suivi de 4 corollaires (corollaires 3.10, 3.11 et 3.12) correspondant à une application du théorème 3.4 pour $r \in \{6, 8, 10\}$.

Théorème 2.32 ([23]). *Soit $r \geqslant 8$ un entier tel que $4 \mid r$. Alors toutes les solutions entières positives de l'équation $x^2 - \frac{1}{5}(2^r - 26) xy + y^2 - 2^r = 0$ sont données par $(x, y) = (u_{n+2} + 5u_{n+1}, u_{n+1} + 5u_n)$ avec $n \geqslant 0$ et $(x, y) = (5u_{n+1} + u_n, 5u_n + u_{n-1})$ avec $n > 0$, où $u_n = F_n\left(\frac{1}{5}(2^r - 26), -1\right)$.*

Ce théorème est suivi d'un corollaire (corollaire 3.13) correspondant à une application du théorème 3.5 pour $r = 8$.

Théorème 2.33 ([23]). *Soit $r \geqslant 9$ un entier tel que $3 \mid r$. Alors toutes les solutions entières positives de l'équation $x^2 - \frac{1}{7}(2^r - 50)xy + y^2 - 2^r = 0$ sont données par $(x, y) = (u_{n+2} + 7u_{n+1}, u_{n+1} + 7u_n)$ avec $n \geqslant 0$ et $(x, y) = (7u_{n+1} + u_n, 7u_n + u_{n-1})$ avec $n > 0$, où $u_n = F_n\left(\frac{1}{7}(2^r - 50), -1\right)$.*

Ce théorème est suivi d'un corollaire (corollaire 3.14) correspondant à une application du théorème 3.6 pour $r = 9$.

Théorème 2.34 ([23]). *Soit $r \geqslant 10$ un entier tel que $10 \mid r$. Alors toutes les solutions entières positives de l'équation $x^2 - \frac{1}{11}(2^r - 122)xy + y^2 - 2^r = 0$ sont données par $(x, y) = (u_{n+2} + 11u_{n+1}, u_{n+1} + 11u_n)$ avec $n \geqslant 0$ et $(x, y) = (11u_{n+1} + u_n, 11u_n + u_{n-1})$ avec $n > 0$, où $u_n = F_n\left(\frac{1}{11}(2^r - 122), -1\right)$.*

Ce théorème est suivi d'un corollaire (corollaire 3.14) correspondant à une application du théorème 3.7 pour $r = 10$.

Posons pour $k \in \mathbb{N}^*$, $(a, b) \in \mathbb{N}^2$ et $u_n = F_n(k; -1)$:

$$\begin{aligned} A^{(a,b)}(k) &= \{(au_{n+2} + bu_{n+1}, au_{n+1} + bu_n) \ / \ n \geqslant 0\}, \\ \widetilde{A}^{(a,b)}(k) &= A^{(a,b)}(k) \cup A^{(b,a)}(k), \\ k_{p,r} &= \frac{2^r - p^2 - 1}{p}. \end{aligned}$$

Soit $\mathcal{C}_p(r)$ la condition sur l'entier r définie pour $p \in \{3, 5, 7, 11\}$ comme suit :

$$\begin{aligned} \mathcal{C}_3(r) &\iff 2 \mid r \text{ et } r > 4, \\ \mathcal{C}_5(r) &\iff 4 \mid r \text{ et } r > 4, \\ \mathcal{C}_7(r) &\iff 3 \mid r \text{ et } r > 4, \\ \mathcal{C}_{11}(r) &\iff 10 \mid r \text{ et } r > 4. \end{aligned}$$

Il est facile de vérifier que pour $p \in \{3, 5, 7, 11\}$, on a $k_{p,r} \in \mathbb{N}^*$ et $k_{p,r} \neq 2$ pourvu que la condition $\mathcal{C}_p(r)$ soit vérifiée. Les théorèmes 3.1, 3.2, 3.3 se résument dans le théorème suivant :

Théorème 2.35. *1. L'ensemble des solutions entières positives de l'équation $x^2 - kxy + y^2 - 1 = 0$ est $A^{(1,0)}(k)$.*

2. L'ensemble des solutions entières positives de l'équation $x^2 - kxy + y^2 - 2^r = 0$ est $2^r A^{(1,0)}(k)$.

3. L'ensemble des solutions entières positives de l'équation $x^2 - (2^{2r} - 2)xy + y^2 - 2^r = 0$ est $\{(u_{n+1}, u_{n-1}) \ / \ n \geqslant 1\}$.

Le théorème suivant est une synthèse des théorèmes 3.4, 3.5, 3.6 et 3.7 :

Théorème 2.36. *Pour $p \in \{3, 5, 7, 11\}$ et pour tout entier r vérifiant la condition $\mathcal{C}_p(r)$ l'ensemble des solutions entières positives de l'équation $x^2 - k_{p,r}xy + y^2 - 2^r = 0$ est $\widetilde{A}^{(1,p)}(k)$.*

En 2012, dans [22], Keskin, Karaatli et Siar ont étudié l'équation diophantienne

$$x^2 - kxy + y^2 + 2^n = 0. \tag{2.23}$$

pour $0 \leqslant n \leqslant 10$ et pour $k \in \mathbb{N}^*$. Pour chacune de ces valeurs de n, ils ont déterminé les valeurs de k pour lesquelles l'équation correspondante admet une infinité de solutions et ils ont de plus déterminé explicitement l'ensemble des solutions pour ces valeurs particulières de n et k.

Le théorème suivant synthétise les résultats du corollaire 1 et des théorèmes 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 et 13 de [22] :

Théorème 2.37. *1.* $\#S\left\{x^2-kxy+y^2+1=0\right\}=\infty \Longleftrightarrow k=3$.

2. $\#S\left\{x^2-kxy+y^2+2=0\right\}=\infty \Longleftrightarrow k=4$.

3. $\#S\left\{x^2-kxy+y^2+4=0\right\}=\infty \Longleftrightarrow k\in\{3,6\}$.

4. $\#S\left\{x^2-kxy+y^2+8=0\right\}=\infty \Longleftrightarrow k\in\{4,6,10\}$.

5. $\#S\left\{x^2-kxy+y^2+16=0\right\}=\infty \Longleftrightarrow k\in\{3,6,18\}$.

6. $\#S\left\{x^2-kxy+y^2+32=0\right\}=\infty \Longleftrightarrow k\in\{4,6,10,14,34\}$.

7. $\#S\left\{x^2-kxy+y^2+64=0\right\}=\infty \Longleftrightarrow k\in\{3,6,18,66\}$.

8. $\#S\left\{x^2-kxy+y^2+128=0\right\}=\infty \Longleftrightarrow k\in\{4,6,10,14,34,46,130\}$.

9. $\#S\left\{x^2-kxy+y^2+256=0\right\}=\infty \Longleftrightarrow k\in\{3,6,18,66,258\}$.

10. $\#S\left\{x^2-kxy+y^2+512=0\right\}=\infty \Longleftrightarrow k\in\{4,6,10,14,34,46,66,130,174,514\}$.

11. $\#S\left\{x^2-kxy+y^2+1024=0\right\}=\infty \Longleftrightarrow k\in\{3,6,18,66,210,258,1026\}$.

Le théorème suivant synthétise les résultats des corollaires $2,3,4,5,6$, du théorème 19, des corollaires $7,8,9,10,11,13,14$ et des théorèmes $20,22,23,24,25,26$ de [22] :

Théorème 2.38. *1.* $S\left\{x^2-3xy+y^2+1=0\right\}=\{(F_{2n+1},F_{2n-1})\ /\ n\geqslant 0\}$.

2. $S\left\{x^2-4xy+y^2+2=0\right\}=\{(u_{n+1}-u_n,u_n-u_{n-1})\ /\ n\geqslant 0\}$ *où* $u_n=F_n(4,-1)$.

3. $S\left\{x^2-3xy+y^2+4=0\right\}=\{(2F_{2n+1},2F_{2n-1})\ /\ n\geqslant 0\}$.

4. $S\left\{x^2-6xy+y^2+4=0\right\}=\{(P_{2n+1},P_{2n-1})\ /\ n\geqslant 0\}$.

5. $S\left\{x^2-4xy+y^2+8=0\right\}=\{(2u_{n+1}-2u_n,2u_n-2u_{n-1})\ /\ n\geqslant 0\}$ *où* $u_n=F_n(4,-1)$.

6. $S\left\{x^2-6xy+y^2+8=0\right\}=\{(3v_{n+1}-v_n,3v_n-v_{n-1})\ /\ n\geqslant 0\}$ *où* $v_n=F_n(6,-1)$.

7. $S\left\{x^2-10xy+y^2+8=0\right\}=\{(w_{n+1}-w_n,w_n-w_{n-1})\ /\ n\geqslant 0\}$ *où* $w_n=F_n(10,-1)$.

8. $S\left\{x^2-3xy+y^2+16=0\right\}=\{(4F_{2n+1},4F_{2n-1})\ /\ n\geqslant 0\}$.

9. $S\left\{x^2-6xy+y^2+16=0\right\}=\{(2P_{2n+1},2P_{2n-1})\ /\ n\geqslant 0\}$.

10. $S\left\{x^2-18xy+y^2+16=0\right\}=\{(u_{2n+1},u_{2n-1})\ /\ n\geqslant 0\}$ *où* $u_n=F_n(4,-1)$.

11. $S\left\{x^2-4xy+y^2+32=0\right\}=\{(4u_{n+1}-4u_n,4u_n-4u_{n-1})\ /\ n\geqslant 0\}$ *où* $u_n=F_n(4,-1)$.

12. $S\left\{x^2-6xy+y^2+32=0\right\}=\{(6v_{n+1}-2v_n,6v_n-2v_{n-1})\ /\ n\geqslant 0\}$ *où* $v_n=F_n(6,-1)$.

13. $S\left\{x^2-10xy+y^2+32=0\right\}=\{(6w_{n+1}-2w_n,6w_n-2w_{n-1})\ /\ n\geqslant 0\}$ *où* $w_n=F_n(10,-1)$.

14. $S\left\{x^2-34xy+y^2+32=0\right\}=\{(p_{n+1}-p_n,p_n-p_{n-1})\ /\ n\geqslant 0\}$ *où* $p_n=F_n(34,-1)$.

15. $S\left\{x^2-14xy+y^2+32=0\right\}=\{(3u_{n+1}-u_n,3u_n-u_{n-1})\ /\ n\geqslant 0\}$ *où* $u_n=F_n(4,-1)$.

16. $S\left\{x^2-46xy+y^2+128=0\right\}=\{(3q_{n+1}-q_n,3q_n-q_{n-1})\ /\ n\in\mathbb{Z}\}$ *où* $q_n=F_n(46,-1)$.

17. $S\left\{x^2-174xy+y^2+512=0\right\}=\{(3r_{n+1}-r_n,3r_n-r_{n-1})\ /\ n\in\mathbb{Z}\}$ *où* $r_n=F_n(174,-1)$.

18. $S\left\{x^2-66xy+y^2+512=0\right\}=\{(9s_{n+1}-s_n,9s_n-s_{n-1})\ /\ n\in\mathbb{Z}\}$ *où* $s_n=F_n(66,-1)$.

19. $S\left\{x^2-210xy+y^2+1024=0\right\}=\{(5t_{n+1}-t_n,5t_n-t_{n-1})\ /\ n\in\mathbb{Z}\}$ *où* $t_n=F_n(210,-1)$.

20. $S\left\{x^2-66xy+y^2+1024=0\right\}=A\cup B$ *avec*
$A=\{(41s_{n+1}-s_n,41s_n-s_{n-1})\ /\ n\in\mathbb{Z}\}$ *et* $B=\{(4\ell_{2n+1},4\ell_{2n-1})\ /\ n\geqslant 0\}$ *où*
$s_n=F_n(66,-1)$ *et* $\ell_n=F_n(8,1)$.

Le théorème 2.38 traite 20 des 48 cas de couples $(n,k)\in\{0,1,2,3,4,5,6,7,8,9,10\}\times\mathbb{N}^*$ décrits au théorème 2.37 pour lesquelles l'équation (2.23) admet une infinité de solutions. Les 28 cas restants étant les équations diophantiennes suivantes

$$\begin{aligned}
x^2-kxy+y^2+64 &= 0,\quad k\in\{3,6,18,66\},\\
x^2-kxy+y^2+128 &= 0,\quad k\in\{4,6,10,14,34,130\},\\
x^2-kxy+y^2+256 &= 0,\quad k\in\{3,6,18,66,258\},\\
x^2-kxy+y^2+512 &= 0,\quad k\in\{4,6,10,14,34,46,130,514\},\\
x^2-kxy+y^2+1024 &= 0,\quad k\in\{3,6,18,258,1026\}.
\end{aligned}$$

Pour tous ces cas, Keskin, Karaatli et Siar affirment que l'ensemble des solutions entières positives de chacune de ces équations peut s'obtenir facilement en utilisant les théorèmes et les corollaires de leur article.

En 2013, dans [23], Keskin, Karaatli et Siar ont étudié l'équation diophantienne

$$x^2 - kxy + y^2 - 2^n = 0. \tag{2.24}$$

pour $0 \leqslant n \leqslant 10$ et pour $k \in \mathbb{N}^*$. Pour chacune de ces valeurs de n, ils ont déterminé les valeurs de k pour lesquelles l'équation correspondante admet une infinité de solutions et ils ont de plus déterminé explicitement l'ensemble des solutions pour ces valeurs particulières de n et k. Enfin, leurs calculs les amènent à formuler une conjecture concernant l'équation diophantienne (2.24).

Le théorème suivant synthétise les résultats du corollaire 1 et des théorèmes 2.1, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.11, 2.12, 2.13 et 2.14 de [23] :

Théorème 2.39. *1.* $\#S\left\{x^2 - kxy + y^2 - 1 = 0\right\} = \infty \iff k > 1.$

2. $\#S\left\{x^2 - kxy + y^2 - 2 = 0\right\} = \varnothing.$

3. $\#S\left\{x^2 - kxy + y^2 - 4 = 0\right\} = \infty \iff k > 1.$

4. $S_1\left\{x^2 - kxy + y^2 - 4 = 0\right\} \neq \varnothing \iff k = 2.$

5. $\#S\left\{x^2 - kxy + y^2 - 8 = 0\right\} = \infty \iff k = 6.$

6. $\#S\left\{x^2 - kxy + y^2 - 16 = 0\right\} = \infty \iff k > 1.$

7. $S_1\left\{x^2 - kxy + y^2 - 16 = 0\right\} \neq \varnothing \iff k \in \{2, 14\}.$

8. $\#S\left\{x^2 - kxy + y^2 - 32 = 0\right\} = \infty \iff k \in \{6, 30\}.$

9. $\#S\left\{x^2 - kxy + y^2 - 64 = 0\right\} = \infty \iff k > 1.$

10. $S_1\left\{x^2 - kxy + y^2 - 64 = 0\right\} \neq \varnothing \iff k \in \{2, 18, 62\}.$

11. $\#S\left\{x^2 - kxy + y^2 - 128 = 0\right\} = \infty \iff k \in \{6, 30, 126\}.$

12. $\#S\left\{x^2 - kxy + y^2 - 256 = 0\right\} = \infty \iff k > 1.$

13. $S_1\left\{x^2 - kxy + y^2 - 256 = 0\right\} \neq \varnothing \iff k \in \{2, 46, 82, 254\}.$

14. $\#S\left\{x^2 - kxy + y^2 - 512 = 0\right\} = \infty \iff k \in \{6, 30, 66, 126, 510\}.$

15. $\#S\left\{x^2 - kxy + y^2 - 1024 = 0\right\} = \infty \iff k > 1.$

16. $\#S_1\left\{x^2 - kxy + y^2 - 1024 = 0\right\} \neq \varnothing \iff k \in \{2, 46, 66, 82, 338, 1022\}.$

Rappelons que pour $k, a, b \in \mathbb{N}$, les ensembles $A^{(a,b)}(k)$ et $\widetilde{A}^{(a,b)}(k)$ ont été définis comme suit :

$$\begin{aligned} A^{(a,b)}(k) &= \{(au_{n+2} + bu_{n+1}, au_{n+1} + bu_n) \ / \ n \geqslant 0\}, \\ \widetilde{A}^{(a,b)}(k) &= A^{(a,b)}(k) \cup A^{(b,a)}(k). \end{aligned}$$

Le théorème suivant synthétise les résultats du théorèmes 3.1, des corollaires 3.6, 3.2, 3.7, 3.10, 3.3, 3.8, 3.13, 3.11, 3.4, 3.14, 3.9, des théorèmes 3.8, 3.9 et des corollaires 3.15, 3.12 et 3.5 [23] :

Théorème 2.40. *1. Pour* $k \geqslant 3$*, on a* $S\left\{x^2 - kxy + y^2 - 1 = 0\right\} = A^{(1,0)}(k).$

2. $S\left\{x^2 - 6xy + y^2 - 8 = 0\right\} = A^{(1,1)}(6).$

3. $S\left\{x^2 - 14xy + y^2 - 16 = 0\right\} = A^{(1,0)}(4).$

4. $S\left\{x^2 - 30xy + y^2 - 32 = 0\right\} = A^{(1,1)}(30).$

5. $S\left\{x^2 - 18xy + y^2 - 64 = 0\right\} = A^{(1,3)}(18).$

6. $S\left\{x^2 - 62xy + y^2 - 64 = 0\right\} = A^{(1,0)}(8).$

7. $S\left\{x^2 - 126xy + y^2 - 128 = 0\right\} = A^{(1,1)}(126).$

8. $S\left\{x^2-46xy+y^2-256=0\right\}=A^{(1,5)}(46)$.
9. $S\left\{x^2-82xy+y^2-256=0\right\}=A^{(1,3)}(82)$.
10. $S\left\{x^2-254xy+y^2-256=0\right\}=A^{(1,0)}(16)$.
11. $S\left\{x^2-66xy+y^2-512=0\right\}=A^{(1,7)}(66)$.
12. $S\left\{x^2-510xy+y^2-512=0\right\}=A^{(1,1)}(510)$.
13. $S\left\{x^2-46xy+y^2-1024=0\right\}=A^{(3,7)}(46)$.
14. $S\left\{x^2-66xy+y^2-1024=0\right\}=A^{(3,5)}(66)$.
15. $S\left\{x^2-82xy+y^2-1024=0\right\}=A^{(1,11)}(82)$.
16. $S\left\{x^2-338xy+y^2-1024=0\right\}=A^{(1,3)}(338)$.
17. $S\left\{x^2-1022xy+y^2-1024=0\right\}=A^{(1,0)}(32)$.

La détermination explicite de l'ensemble des solutions des équations diophantiennes restantes

$$\begin{aligned} x^2-kxy+y^2-32 &= 0,\ k\in\{6\},\\ x^2-kxy+y^2-128 &= 0,\ k\in\{6,30\},\\ x^2-kxy+y^2-512 &= 0,\ k\in\{6,30,126\}, \end{aligned}$$

n'a pas été effectuée par Keskin, Siar et Karaartli. Dans leur article [23], ils affirment simplement que l'ensemble des solutions entières positives de chacune de ces équations pourrait être effectivement explicité facilement en utilisant les théorèmes précédents.

2.4.3 Preuve de la conjecture de Keskin, Siar et Karaatli

En 2016, dans [6] nous avons donné une réponse positive à la conjecture de Keskin, Siar et Karaatli. Nous avons aussi établi un résulat analogue pour l'équation diophantienne $x^2+y^2-kxy=-2^n$.

Théorème 2.41. *Soit l'équation diophantienne*

$$x^2+y^2-kxy=2^n. \tag{2.25}$$

1. *On suppose que n impair et $n\geqslant 3$.*
   i. *Si $k>2^n-2$, alors l'équation (2.25) n'admet pas de solution entière positive.*
   ii. *Si l'équation (2.25) admet une solution entière positive, alors k est pair et $k\leqslant 2^n-2$.*
2. *On suppose n pair $n\geqslant 2$.*
   i. *Si $k>2^n-2$, alors l'équation (2.25) n'admet pas de solution entière impaire.*
   ii. *Si l'équation (2.25) admet une solution positive impaire, alors k est pair et $k\leqslant 2^n-2$.*

Démonstration. Supposons que n est un entier impair, avec $n>2$. Il est clair que si (x,y) est une solution positive de l'équation diophantienne $x^2-kxy+y^2=2^n$, alors x et y sont de même parité (si x est pair $y^2=-x^2+kxy+2^n$ est à son tour pair, par suite y est pair. Si x est impair, $-x^2+2^n=y(-kx+y)$ est à son tour impair, d'où y est impair).
Si x et y sont impairs, alors k est pair. En effet $kxy=x^2+y^2+2^n$ est pair, d'où k est pair. Supposons x et y pairs, $x=2X$ et $y=2Y$ l'équation (2.25) donne

$$X^2-kXY+Y^2=2^{n-2}.$$

De la même manière, si X est pair alors Y est pair aussi, et comme n est impair on refait le même raisonnement avec X et Y dans l'équation précédente jusqu'a épuiser toutes les puissances de 2 dans x et y pour obtenir à la fin l'équation

$$X^2 + Y^2 - kXY = 2^r.$$

avec X, Y et r des entiers positifs impairs ce qui implique que k est pair.
En effectuant le changement de variables $u =\mid x - \frac{k}{2}y \mid$, $v = y$ et $d = (\frac{k^2}{4} - 1)$
l'équation (2.25) devient

$$u^2 - dv^2 = 2^n. \tag{2.26}$$

Avec u et v positifs.car k est pair. Si $k = 2$ et n impair, l'équation précédente donne $u^2 = 2^n$, ce qui est impossible, donc $k > 2$ ce qui donne $d > 1$.
L'équation de Pell $x^2 - dy^2 = 1$ avec $d = \left(\frac{k^2}{2} - 1\right)$ a pour solution fondamentale $\left(\frac{k}{2} + \sqrt{\frac{k^2}{2} - 1}\right)$.
Si l'équation (2.26) admettait une solution positive avec n impair $n > 2$, alors l'équation (2.25) admet à son tour une solution positive.
Si $u_0 + v_0\sqrt{d}$ est la solution fondamentale d'une classe K de solutions de l'équation (2.26), le lemme 2.22 nous donne

$$0 \leqslant v_0 \leqslant \frac{1}{\sqrt{2\left(\frac{k}{2} + 1\right)}}\sqrt{2^n}$$

$v_0 \neq 0$, sinon $u_0^2 = 2^n$ ce qui est impossible vu que n est impair,
donc $v_0 \geqslant 1$, ce qui donne

$$\frac{1}{\sqrt{2\left(\frac{k}{2} + 1\right)}}\sqrt{2^n} \geqslant 1,$$

par suite $k \leqslant 2^n - 2$.

Supposons que n est un entier pair positif et (x, y) est une solution de l'équation (2.25), il est clair que si x et y sont tous les deux impairs k est pair.
En faisant les changements de variables $u =\mid x - \frac{k}{2}y \mid$, $v = y$ et $d = \frac{k^2}{4} - 1$ on obtient l'équation (2.26)

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

Comme $k \neq 0$ et k est pair donc $k \geqslant 2$ d'où d est un entier $d \geqslant 0$. comme $k > 2^n - 2$ et n pair, alors nécessairement $k > 2$ par conséquent $d > 1$,le lemme 2.22 donne

$$0 \leqslant v \leqslant \frac{1}{\sqrt{2\left(\frac{k}{2} + 1\right)}}\sqrt{2^n}, \tag{2.27}$$

or $\left(\frac{k}{2} + \sqrt{\frac{k^2}{2} - 1}\right)$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$ avec $d = (\frac{k^2}{4} - 1)$.
Si $v = 0$, alors l'équation (2.26) donne $u = 2^{\frac{n}{2}}$, par suite les solutions qui sont dans la même classe que $(2^{\frac{n}{2}}, 0)$ sont paires,.alors les solutions de (2.25) sont aussi paires Comme on a supposé qu'il existe des solutions impairs on peut supposer que $v \geqslant 1$. L'inégalité (2.27), donne

$$\frac{1}{\sqrt{2\left(\frac{k}{2} + 1\right)}}\sqrt{2^n} \geqslant 1,$$

c'est-à-dire

$$k \leqslant 2^n - 2.$$

□

2.4.4 Applications

En procédant de la même manière, on obtient le théorème analogue suivant

Théorème 2.42. *Soit l'équation*

$$x^2 - kxy + y^2 = -2^n \tag{2.28}$$

1. *supposons n impair et $n > 2$.*
   - *Si $k > 2^n + 2$, l'équation (2.28) n'admet pas de solution positive entière.*
   - *Si l'équation (2.28) admet des solutions alors k est pair et $k \leqslant 2^n + 2$.*
2. *Supposons n pair et $n \geqslant 2$.*
   - *Si $k > 2^n + 2$, l'équation (2.28) n'admet pas de solution positives impaires.*
   - *Si l'équation (2.28) admet une solution positive impaire, alors $k \leqslant 2^n + 2$ et k est pair non divisible par 4.*

Démonstration. Soit n un entier impair $n > 2$.
On fait le même raisonnement comme dans la preuve du théorème 2.41. Si (x, y) est solution positive de (2.28), les entiers x et y sont de même parité. Si x et y sont impairs alors k est pair
Supposons x et y pairs $x = 2X$ et $y = 2Y$, l'équation (2.28) donne

$$X^2 - kXY + Y^2 = 2^{n-2}. \tag{2.29}$$

De la même manière, si X est pair Y l'est aussi, et comme n est impair, on utilise le même procédé avec X et Y dans (2.29) et ainsi de suite jusqu'a épuiser toutes les puissances de 2 dans x et y pour obtenir l'équation

$$X^2 + Y^2 - kXY = 2^r$$

avec X, Y et r des entiers positifs impairs ce qui implique que k pair.
En faisant les mêmes changements de variables que dans le théorème 2.41, $u =\mid x - \frac{k}{2}y \mid$, $v = y$ et $d = \left(\frac{k^2}{4} - 1\right)$, l'équation devient

$$u^2 - dv^2 = -2^n. \tag{2.30}$$

Puisque k est pair, u et v sont des entiers positifs.
Si $k = 2$, l'équation devient $u^2 = -2^n$, qui est impossible, d'où $k > 2$ il s'en suit que $d > 1$.
$\left(\frac{k}{2} + \sqrt{\frac{k^2}{2} - 1}\right)$ étant la solution fondamentale de $x^2 - dy^2 = 1$.Si l'équation admet une solution positive et n pair, alors (2.28) admet une solution positive.
Si $u_0 + v_0\sqrt{d}$ est la solution fondamentale d'une classe de solutions K,de l'équation 2.30, alors le lemme 2.24 donne

$$0 < v_0 \leqslant \frac{1}{\sqrt{2\left(\frac{k}{2} - 1\right)}}\sqrt{2^n},$$

Comme dans la preuve du théorème 2.41, on peut supposer que $v_0 \geqslant 1$. Par conséquent

$$k \leqslant 2^n + 2.$$

Supposons n pair non nul et (x, y) solution de l'équation (2.28), alors le même raisonnement donne k pair et

$$k \leqslant 2^n + 2.$$

Supposons n pair non nul, (x, y) solution impaire de l'équation

$$x^2 - kxy + y^2 = -2^n$$

en réduisant modulo 4 on obtient

$$x^2 - kxy + y^2 \equiv 0 \pmod 4 \tag{2.31}$$

Comme x et y sont impairs, en prenant $x = 2\ell_1 + 1$ et $y = 2\ell_2 + 1$ dans (2.31) on obtient

$$2 - k(2\ell_1 + 2\ell_2 + 1) \equiv 0 \pmod 4$$

$$k(2(\ell_1 + \ell_2) + 1) \equiv 2 \pmod 4.$$

D'où nécessairement k est pair , $k = 2\ell$ avec ℓ non divisible par 2. □

Remarque 2.43. *Dans le théorème 2.41, la borne $k = 2^r - 2$ est atteinte grâce aux théorèmes 2.29 et 2.30.*

Remarque 2.44. *Dans le théorème 2.42 la borne $k = 2^r + 2$ est atteinte grâce aux théorèmes suivants*

Théorème 2.45. *Soit r un entier impair $r \geqslant 1$, les solutions positives de l'équation*

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

sont données par

$$(x, y) = (F_{n+1}(2^r + 2, -1) - F_n(2^r + 2, -1), F_n(2^r + 2, -1) - F_{n-1}(2^r + 2, -1)),\ n \geqslant 0.$$

Théorème 2.46 ([22])**.** *Soit r un entier $r \geqslant 1$, les solutions positives de l'équation*

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

sont données par

$$(x, y) = (F_{n+1}(2^{2r} + 2, -1) - F_n(2^{2r} + 2, -1), F_n(2^{2r} + 2, -1) - F_{n-1}(2^{2r} + 2, -1)),\ n \geqslant 0.$$

Théorème 2.47. *1. Soit n un entier impair, p un nombre premier impair tel que $\left(\frac{2}{p}\right) = -1$. Si l'équation*

$$x^2 - kxy + y^2 = 2^n,$$

admet une solution positive, alors $\frac{k}{2} \not\equiv \pm 1 \pmod p$. En particulier, k est un multiple de 3.

2. Soit n un entier impair et p un nombre premier tel que $\left(\frac{2}{p}\right) = +1$ et $p \equiv 3 \pmod 4$. Si l'équation

$$x^2 - kxy + y^2 = -2^n$$

admet une solution, alors $\frac{k}{2} \not\equiv \pm 1 \pmod p$.

Démonstration. 1. Si n est un entier impair et l'équation $x^2 - kxy + y^2 = +2^n$ admet des solutions, alors d'aprés le théorème 2.41, k est pair et l'équation

$$u^2 - \left(\frac{k^2}{4} - 1\right) v^2 = 2^n \tag{2.32}$$

obtenue par les changements de variables $u = \mid x - \frac{k}{2}y \mid$ et $v = y$ admet à son tour des solutions.

Si $\frac{k}{2} \equiv \pm 1 \pmod{p}$, alors $\frac{k^2}{4} - 1 \equiv 0 \pmod{p}$; en réduisant l'équation (2.32) modulo p et en injectant l'hypothèse $(\frac{k^2}{4} - 1) \equiv 0 \pmod{p}$ on obtient :

$$u^2 \equiv 2^n \pmod{p} \tag{2.33}$$

d'où

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

Autrement dit

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

Ce qui contredit l'hypothèse $\left(\frac{2}{p}\right) = -1$ et n impair.
Conclusion $\frac{k}{2} \not\equiv \pm 1 \pmod{p}$. En particulier, puisque $\left(\frac{2}{3}\right) = -1$, alors $\frac{k}{2} \not\equiv \pm 1 \pmod{3}$, autrement dit $\frac{k}{2} \equiv 0 \pmod{3}$. Par conséquent k est nécessairement un multiple de 3.

2. Si n est un entier impair et l'équation

$$x^2 - kxy + y^2 = -2^n \tag{2.34}$$

admet des solutions, alors d'après le théorème 2.42, k est pair et l'équation

$$u^2 - \left(\frac{k^2}{4} - 1\right) v^2 = -2^n \tag{2.35}$$

obtenue après les changements de variables $u = \mid x - \frac{k}{2}y \mid$ et $v = y$ admet à son tour des solutions. Si on suppose que $\frac{k}{2} \equiv \pm 1 \pmod{p}$, alors $\frac{k^2}{4} - 1 \equiv 0 \pmod{p}$.
En réduisant l'équation (2.35) modulo p et en injectant l'hypthèse $\left(\frac{k^2}{4} - 1\right) \equiv 0 \pmod{p}$, on obtient

$$u^2 \equiv -2^n \pmod{p}.$$

Autrement dit

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

Or

$$\begin{aligned}\left(\frac{(p-1)2^n}{p}\right) &= \left(\frac{p-1}{p}\right)\left(\frac{2^n}{p}\right) \\ &= \left(\frac{p-1}{p}\right)\left(\frac{2}{p}\right)^n \\ &= \left(\frac{-1}{p}\right) 1^n = 1.\end{aligned}$$

□

Chapitre 3

Polynômes à coefficients entiers dont les valeurs sont des puissances d'entiers

"*Est rigoureuse toute démonstration, qui, chez tout lecteur suffisamment instruit et préparé, suscite un état d'évidence qui entraîne l'adhésion*"
René Thom

3.1 Introduction

Plusieurs auteurs ont étudié l'existence des solutions dans $\mathbb{Z}$ de l'équation diophantienne

$$y^m = P(x),$$

où $P(x)$ est un polynôme à coefficients dans $\mathbb{Q}$, et m est entier tel que $m \geqslant 2$. Si $P(x) \in \mathbb{Z}[x]$, est irréductible et de $\deg P \geqslant 5$, l'équation ci-dessus est appelée hyperelliptique si $m = 2$ et superelliptique si $m \geqslant 3$. En 1969, Baker [3] a démontré un théorème qui fournit une majoration du nombre de solutions entières de l'équation hyperelliptique lors que $P(x)$ possède au moins trois racines simples, et de l'équation superelliptique si $P(x) \in \mathbb{Z}[x]$ possède au moins deux racines simples. En améliorant l'estimation de Baker, Tijdeman [52] a prouvé en 1976 que l'équation de Catalan $x^p - y^q = 1$, admet un nombre fini de solutions en entiers $p > 1$, $q > 1$, $x > 1$, $y > 1$.

En supposant que $y^m - P(x)$ est irréductible dans $\mathbb{Q}[x, y]$, où P est un polynôme unitaire, et $\text{pgcd}(m, \deg P) > 1$, Masser [32] a étudié l'équation $y^m = P(x)$ dans le cas particulier $m = 2$ et $\deg P = 4$. En posant $P(x) = x^4 + ax^3 + bx^2 + cx + d$ où $P(x)$ n'est pas un carré parfait, il a été prouvé que pour $H \geqslant 1$ et $X(H)$ défini comme le maximum des $|x|$ pris sur toutes les solutions entières de toutes les équations $y^2 = P(x)$ avec $\max\{|a|, |b|, |c|, |d|\} \leqslant H$, il existe des constantes réelles $k > 0$ et K tels que $kH^3 \leqslant X(H) \leqslant KH^3$. Walsh [54] a obtenu une borne effective pour les solutions entières dans le cas général. Dans [42], Poulakis a donné une méthode élémentaire pour calculer les solutions de l'équation $y^2 = P(x)$, où P est un polynôme unitaire de degré 4 qui n'est pas un carré parfait. Quelques années plus tard, Szalay [48] a établi une généralisation concernant l'équation $y^q = P(x)$, où P est un polynôme unitaire et q divise $\deg P$.

Si $\alpha_1, \alpha_2, ..., \alpha_r$ sont les racines de $P(x)$ d'ordres de multiplicité $e_1, e_2, ..., e_r$. respectivement, étant donnée un entier $m \geqslant 3$, on définit, pour chaque $i = 1, ..., r$,

$$m_i = \frac{m}{\text{pgcd}(e_i, m)} \in \mathbb{N}.$$

LeVeque [28] a prouvé que l'équation superelliptique $y^m = P(x)$ ne peut avoir une infinité de solutions dans $\mathbb{Q}$, que si $(m_1, m_2, ..., m_r)$ est une des permutations suivantes $(2, 2, 1, ..., 1)$, $(t, 1, 1, ..., 1)$ avec $t \geqslant 1$. En 1995, Voutier [53] a donné de nouvelles améliorations des bornes de la taille des

solutions (x_0, y_0) de l'équation superelliptique avec $x_0 \in \mathbb{Z}$ et $y_0 \in \mathbb{Q}$ avec les mêmes conditions prises par LeVeque. Etant donné un polynôme $P(x) \in \mathbb{Z}[x]$ et un entier $q \geqslant 2$, il est naturel de poser la question suivante : dans quels cas l'équation

$$y^q - P(x) = 0$$

admet une infinité de solutions (x_0, y_0) avec $x_0 \in \mathbb{Z}$ et $y_0 \in \mathbb{Q}$? Il est clair que c'est le cas quand $P(x) = (R(x))^q$ pour un certain polynôme $R(x) \in \mathbb{Q}[x]$. C'est cette question qui nous sers comme motivation principale.

En 1913, Grösch a résolu un problème, posé par Jentzsch [24], en prouvant que si pour un polynôme $P(x)$ à coefficients entiers, $P(\alpha)$ est le carré d'un entier pour toute valeur entière α de x, alors $P(x)$ est le carré d'un polynôme à coeficients entiers (ie $P(x) = (Q(x))^2$ pour un certain$Q(x)$) Quelques années plus tard, Kojima [24], Fuchs [10], et Shapiro [46] ont prouvé d'autres résultas encore plus généraux. En particulier, Shapiro a prouvé que si $P(x)$ et $Q(x)$ sont des polynômes, de degrés p et q respectivement, qui ne prennent que des valeurs entières pour des valeurs entières de x, avec $P(n)$ de la forme $Q(m)$ pour un nombre infini de blocs d'entiers consécutifs de longueur au moins $\frac{p}{q} + 2$, alors il existe un polynôme $R(x)$ tel que $P(x) = Q\left(R(x)\right)$.

3.2 Hauteur d'un polynôme

Définition 3.1. *La hauteur d'un polynôme*

$$P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$$

est le réel positif défini par

$$H(P) = \max_{i=0,\ldots,p} |a_i|$$

où $|a_i|$ est le module de $a_i \in \mathbb{C}$ pour $i = 0, ..., p$.

Exemple 3.2. $P(x) = 1 + 2x - 4x^2 + x^3$, $H(P) = 4$.
$P(x) = 2 - ix + (2 + i)x^2$, $H(P) = \sqrt{5}$.

Proposition 3.3. *Soient $P\left(x\right)$ et $Q(x)$ deux polynômes non nuls dans $\mathbb{Z}[x]$ de degrés p et q respectivement, alors on a*

1. $H(P) \geqslant 1$.
2. $H(P') \leqslant pH(P)$.
3. $H(P + Q) \leqslant H(P) + H(Q)$.
4. $H(PQ) \leqslant (1 + p + q)H(P)H(Q)$.

Démonstration. 1. Soit $P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, $P(x)$ non nul, donc il existe $a_i \in \mathbb{Z}$ tel que $a_i \neq 0$ par suite $H(P) \geqslant |a_i| \geqslant 1$.

2. Soit $P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ donc $P^{'}(x) = a_p p x^{p-1} + a_{p-1}(p-1)x^{p-2} + \cdots + a_1 \in \mathbb{Z}[x]$ ce qui donne

$$pH(P) = \max_{i=0,\ldots,p} |pa_i| \geqslant \max_{i=1,\ldots,p} |ia_i| = H(P').$$

3. Soient $P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_1 x + a_0$ et $Q(x) = b^q x^q + b_{q-1}x^{q-1} + \cdots + b_0$ dans $\mathbb{Z}[x]$. Alors

$$P(x) + Q(x) = \sum_{i=0}^{\max(p,q)} (a_i + b_i)x^i.$$

Par suite,

$$H(P+Q) = \max_{i=0,\ldots,\max(p,q)} |a_i + b_i| \leqslant \max_{i=0,\ldots,p} |a_i| + \max_{i=0,\ldots,q} |b_i| = H(P) + H(Q).$$

Le coefficient de x^k dans le produit de $P(x) = a_p x^p + a_{p-1}x^{p-1} + \cdots + a_0$ et $Q(x) = b^q x^q + b_{q-1}x^{q-1} + \cdots + b_0$ est donné par

$$x_k = \sum_{i+j=k} a_i b_j.$$

Or

$$\begin{aligned}\left|\sum_{i+j=k} a_i b_j\right| &\leqslant \sum_{i+j=k} |a_i||b_i| \leqslant \sum_{i+j=k} H(P)H(Q) \\ &\leqslant H(P)H(Q) \sum_{i+j=k} 1 \\ &\leqslant H(P)H(Q)(1+k) \\ &\leqslant H(P)H(Q)(1+p+q).\end{aligned}$$

D'où le résultat

$$H(PQ) \leqslant (1+p+q)H(P)H(Q).$$

□

3.3 Fonction algébrique

Définition 3.4. *Une fonction algébrique est une fonction $y = f(x)$ qui satisfait une équation du type*

$$a_0(x) + a_1(x)y + a_2(x)y^2 + \cdots + a_n(x)y^n = 0$$

où $a_0(x)$, $a_1(x)$, $a_2(x), \ldots, a_n(x) \in \mathbb{C}[x]$.

Exemple 3.5.
- *Une fonction polynomiale est une fonction algébrique qui vérifie $a_0(x)+y = 0$.*
- *Une fonction rationnelle est une fonction algébrique qui vérifie $a_0(x)+a_1(x)y = 0$, $a_1(x) \neq 0$.*
- *Pour tout polynôme $p(x)$, la fonction $y = \sqrt[n]{p(x)}$ est une fonction algébrique.*
- *L'inverse d'une fonction algébrique est une fonction algébrique.*
- *Une fonction qui n'est pas algébrique est dite transcendante comme $\exp x$, $\tan x$ et $\ln x$. Le composé de deux fonctions transcendantes peut donner une fonction algébrique comme*

$$\cos(\arcsin x) = \sqrt{1-x^2}.$$

Le lemme suivant est un résultat qu'on peut trouver dans [43].

Lemme 3.6. *Soit $f(x) \in \mathbb{R}[x]$ un polynôme unitaire. Si $t \geqslant 1 + H(f)$, alors $f(t) > 0$.*

Démonstration. Soit $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$.

En écrivant $f(t)$ sous la forme $f(t) = t^{n-1}\left(t + \left(a_{n-1} + \frac{a_{n-2}}{t} \cdots + \frac{a_1}{t^{n-2}} + \frac{a_0}{t^{n-1}}\right)\right)$, on aura

$$\begin{aligned}\left|a_{n-1} + \frac{a_{n-2}}{t} \cdots + \frac{a_1}{t^{n-2}} + \frac{a_0}{t^{n-1}}\right| &\leqslant \sum_{i=0}^{n-1} |a_i| \left|\left(\frac{1}{t}\right)^{n-1-i}\right| \\ &\leqslant H(f) \sum_{i=0}^{n-1} \left|\left(\frac{1}{t}\right)^{n-1-i}\right| \\ &\leqslant H(f) \frac{1 - \left(\frac{1}{t}\right)^n}{1 - \left(\frac{1}{t}\right)} \\ &\leqslant H(f) \frac{t}{t-1} < t.\end{aligned}$$

On en conclut que

$$t + \left(a_{n-1} + \frac{a_{n-2}}{t} + \cdots + \frac{a_1}{t^{n-2}} + \frac{a_0}{t^{n-1}}\right) > 0.$$

Par suite $f(t) > 0$. □

Le lemme suivant nous sera utile, sa preuve est implicite dans la preuve du seul lemme de l'article [46].

Lemme 3.7. *Soit $f(x)$ une branche d'une fonction algébrique réelle et régulière pour tout $x > x_0$, pour un certain réel x_0, et satisfaisant $|f(x)| < Cx^\alpha$ où $C > 0$ et $\alpha > 0$. Alors*

$$\lim_{x \longrightarrow +\infty} f^{(r+1)}(x) = 0,$$

où r est le plus petit entier supérieur ou égal à α.

Nous établissons maintenant une majoration des racines d'une classe particulière de fonctions algébriques.

Proposition 3.8. *Soit $P(x)$ un polynôme de degré p à coefficients entiers , et soit $f(x)$ une branche d'une fonction algèbrique définie par l'équation $y^q = P(x)$ où q est un entier tel que $q \geqslant 1$. Pour tout entier $k \geqslant 2$, $R_k(x) = q^k f(x)^{kq-1} f^{(k)}(x)$ est un polynôme à coefficients entiers tel que $\deg R_k \leqslant k(p-1)$ et*

$$H(R_k) \leqslant (k-1)! p q^{k-1} H(P)^k \prod_{j=2}^{k} (jp - j + 1)^2.$$

Démonstration. En dérivant $f^q = P$ par rapport à x, on obtient $q f^{q-1} f' = P'$. Comme $\deg P' = p - 1$ et $H(P') \leqslant pH(P)$ (d'aprés la propriété 2) de la proposition 3.3. Considérons maintenant $R_k = q^k f^{kq-1} f^{(k)}$ et prouvons le résultat par récurrence sur k.
Pour le cas $k = 2$, On dérive $q f^{q-1} f' = P'$ par rapport à x pour avoir

$$q f^{q-1} f'' + q(q-1) f^{q-2} f' f' = P''$$

En multipliant les deux membres de l'équation par $q f^q$, on aura

$$\begin{aligned} q^2 f^{2q-1} f'' + (q-1)(q f^{q-1} f')(q f^{q-1} f') &= q f^q P'' \\ q^2 f^{2q-1} f'' + (q-1) P' P' &= q P P''. \end{aligned}$$

Ceci donne

$$R_2 = q^2 f^{2q-1} f'' = q P P'' - (q-1) P' P'.$$

Donc on a

$$\begin{aligned}\deg R_2 &\leqslant \max\{p+\deg P'', \deg P'+\deg P'\}\\ &= \max\{p+(p-1)-1, p-1+p-1\}\\ &= 2(p-1).\end{aligned}$$

Et

$$\begin{aligned}H(R_2) &\leqslant qH(PP'')+(q-1)H(P'P')\\ &\leqslant q(1+p+\deg P'')H(P)H(P'')+q(1+\deg P'+\deg P')H(P')H(P')\\ &\leqslant q(1+p+p-2)H(P)[\deg P'H(P')]+q(1+2p-2)[pH(P)]^2\\ &\leqslant q(2p-1)H(P)(p-1)[pH(P)]+q(2p-1)[pH(P)]^2\\ &\leqslant pq(2p-1)H(P)^2[(p-1)+p]\\ &\leqslant pqH(P)^2(2p-1)^2.\end{aligned}$$

On conclut que la propriété est vraie pour le cas $k=2$.
Nous supposons que le résultat est vrai pour un certain entier $k \geqslant 2$. On dérivant $R_k = q^k f^{kq-1} f^{(k)}$ par rapport à x, on obtient

$$q^k f^{kq-1} f^{(k+1)} + q^k(kq-1)f^{kq-2}f' f^{(k)} = R'_k.$$

Puis en multipliant les deux membres de l'équation par qf^q, nous obtenons

$$\begin{aligned}q^{k+1} f^{[k+1]q-1} f^{(k+1)} + (kq-1)[qf^{q-1}f'][q^k f^{kq-1} f^{(k)}] &= qf^q R'_k\\ q^{k+1} f^{[k+1]q-1} f^{(k+1)} + (kq-1)P'R_k &= qPR'_k.\end{aligned}$$

Ceci donne

$$R_{k+1} = q^{k+1} f^{[k+1]q-1} f^{(k+1)} = qPR'_k - (kq-1)P'R_k.$$

par hypothèse, on a $\deg R_k \leqslant k(p-1)$. D'où

$$\begin{aligned}\deg R_{k+1} &\leqslant \max\{p+\deg R_k{}', \deg P'+\deg R_k\}\\ &\leqslant \max\{p+\deg R_k-1, p-1+\deg R_k\}\\ &\leqslant p-1+\deg R_k\\ &\leqslant p-1+k(p-1)\\ &\leqslant (k+1)(p-1).\end{aligned}$$

De plus,

$$\begin{aligned}H(R_{k+1}) &\leqslant qH(PR_k{}')+(kq-1)H(P'R_k)\\ &\leqslant kq(1+p+\deg R_k{}')H(P)H(R_k{}')+kq(1+\deg P'+\deg R_k)H(P')H(R_k)\\ &\leqslant kq(p+\deg R_k)H(P)\,[\deg R_k H(R_k)]+kq(p+\deg R_k)[pH(P)]H(R_k)\\ &\leqslant kq(p+\deg R_k)^2 H(P)H(R_k).\end{aligned}$$

Par hypothèse, on a $\deg R_k \leqslant k(p-1)$ et $H(R_k) \leqslant (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp-j+1)^2$. Par suite

$$\begin{aligned} H(R_{k+1}) &\leqslant kq\,(p+k(p-1))^2\, H(P)(k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp-j+1)^2 \\ &\leqslant k!pq^k H(P)^{k+1} \prod_{j=2}^{k+1}(jp-j+1)^2. \end{aligned}$$

Ce qui prouve le résultat. □

Corollaire 3.9. *Soit $P(x)$ un polynôme de degré p à coefficients entiers, et soit $f(x)$ une branche d'une fonction algèbrique définie par l'équation $y^q = P(x)$ où q est un entier plus grand que 1. Si β est un zéro réel de $f^{(k)}(x)$ pour tout entier $k \geqslant 2$ tel que $\beta > 1 + H(P)$, alors*

$$\beta \leqslant 1 + (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp-j+1)^2.$$

Démonstration. Soit β une racine de $f^{(k)}(x)$ tel que $\beta > 1 + H(P)$. Si $f(\beta) = 0$, alors $0 = f(\beta)^q = P(\beta)$ et $\beta \leqslant 1 + H(P)$ d'aprés le Lemme 3.6. On conclut que β n'est pas une racine de $f(x)$.

Comme β est une racine du polynôme $R_k = q^k f^{kq-1} f^{(k)}$, on conclut d'aprés le lemme 3.6 et le lemme 3.8 que

$$\beta \leqslant 1 + H(R_k) \leqslant 1 + (k-1)!pq^{k-1}H(P)^k \prod_{j=2}^{k}(jp-j+1)^2.$$

□

Soit Δ l'opérateur aux différences sur $\mathbb{C}[x]$ défini par

$$\Delta f(x) = f(x+1) - f(x).$$

Lemme 3.10. *Pour tout entier $k \geqslant 1$, on a*

$$\Delta^k f(x) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i f(x+k-i).$$

Démonstration. Première méthode :
Nous montrons ce résultat par récurrence. Pour le cas $k = 1$, on a

$$\Delta f(x) = f(x+1) - f(x) = \sum_{i=0}^{1} \binom{1}{i} (-1)^i f(x+1-i)$$

Supposons que le résultat est vrai pour $k \geqslant 1$. Donc par hypothèse, on a

$$\begin{aligned} \Delta^{k+1} f(x) &= \Delta^k f(x+1) - \Delta^k f(x) \\ &= \sum_{i=0}^{k} \binom{k}{i} (-1)^i f(x+1+k-i) - \sum_{j=0}^{k} \binom{k}{j} (-1)^j f(x+k-j) \end{aligned}$$

Par suite,

$$\begin{aligned}\Delta^{k+1}f(x) &= f(x+k+1)+\sum_{i=1}^{k}\binom{k}{i}(-1)^i f(x+1+k-i)\\ &\qquad -\sum_{j=0}^{k-1}\binom{k}{j}(-1)^j f(x+k-j)-(-1)^k f(x)\\ &= f(x+k+1)+\sum_{i=1}^{k}\binom{k}{i}(-1)^i f(x+1+k-i)\\ &\qquad -\sum_{i=1}^{k}\binom{k}{i-1}(-1)^{i-1} f(x+k-i+1)-(-1)^k f(x)\\ &= f(x+k+1)+\sum_{i=1}^{k}\left[\binom{k}{i}+\binom{k}{i-1}\right](-1)^i f(x+1+k-i)+(-1)^{k+1}f(x)\\ &= f(x+k+1)+\sum_{i=1}^{k}\binom{k+1}{i}(-1)^i f(x+1+k-i)+(-1)^{k+1}f(x)\\ &= \sum_{i=0}^{k+1}\binom{k+1}{i}(-1)^i f(x+1+k-i).\end{aligned}$$

Deuxième Méthode :
Cosidérons les deux opérateurs E et I définis pour tout $f\in\mathbb{C}[x]$ par

$$E(f)(x)=f(x+1) \text{ et } I(f)(x)=f(x).$$

Alors pour tout $f\in\mathbb{C}[x]$ on a $\Delta f=(E-I)\,f$. Par suite, pour tout entier positif k,

$$\Delta^k=(E-I)^k.$$

Sachant que les deux opérateurs E et I commutent, en utilisant la formule du binôme on obtient

$$\Delta^k=(E-I)^k=\sum_{i=0}^{k}\binom{k}{i}(-I)^i(E)^{k-i}=\sum_{i=0}^{k}\binom{k}{i}(-1)^i(E)^{k-i}.$$

Par suite

$$\left(\Delta^k f\right)(x)=\sum_{i=0}^{k}\binom{k}{i}(-1)^i f(x+k-i).$$

Ce qui achève la preuve. □

3.4 Résultat principal

En 1957, Shapiro a montré que si les valeurs d'un polnôme $P(x)$ à coefficients entiers pour x appartenant à un nombre infini de blocs d'entiers consécutifs, coincident avec celles d'un polynôme $Q(x)$, alors $P(x)=Q(R(x))$ où $R(x)$ est un polynôme à coefficients entiers. Le théorème suivant donne un énnoncé comparable au résultat de Shapiro mais pour un nombre fini de blocs.

Théorème 3.11. *[5] Soit $P(x)=a_px^p+a_{p-1}x^{p-1}+\cdots+a_0\in\mathbb{Z}[x]$, $a_p>0$, on suppose que p admet un diviseur $q\geqslant 2$ Supposons qu'il existe des entiers n_0,et m_i,où $i=0,1,...,\frac{p}{q}+1$, tels que*

$P(n_0+i)=m_i{}^q$ *avec*

$$n_0 > 1+\left(\frac{p}{q}+1\right)!pq^{\frac{p}{q}+1}H(P)^{\frac{p}{q}+2}\prod_{j=2}^{\frac{p}{q}+2}(jp-j+1)^2.$$

Soit

$$M:=\sum_{i=0}^{\frac{p}{q}+1}\binom{\frac{p}{q}+1}{i}\left|m_{\frac{p}{q}+1-i}\right|.$$

S'il existe au moins M blocs d'entiers n_k+i, $i=0,\dots,\frac{p}{q}+1$ tel que $n_k>n_{k-1}+\frac{p}{q}+1$ pour tout $k=1,\dots,M$ et $P(n_k+i)=m_{k,i}^q$ pour tout $k=1,\dots,M$ et $i=0,\dots,\frac{p}{q}+1$ pour certains entiers $m_{k,i}$ alors il existe un polynôme $R(x)\in\mathbb{Z}[x]$ tel que $P(x)=(R(x))^q$.

Démonstration. Notons par $x=\phi(y)$ la branche de la fonction algébrique de l'inverse du polynôme $y=x^q$, c'est-à-dire , $\phi(y)=y^{\frac{1}{q}}$. Alors $\phi(y)$ est positive et ne possède pas de singularités pour tout $y\geqslant 0$.
Posons $f(x)=\phi\left(P(x)\right)$. Alors $f(x)$ est asymptotiquement égale à $a_p^{\frac{1}{q}}x^{\frac{p}{q}}$, et $f(n)=\pm m$ pour tout n vérifiant $P(n)=m^q$.
Nous montrons par l'absurde que $f(x)$ est un polynôme.
Supposons que $f(x)$ n'est pas un polynôme. Alors $f^{\left(\frac{p}{q}+2\right)}(x)$ n'est pas le polynôme nul. D'aprés le corollaire 3.9, toute racine réelle β de $f^{\left(\frac{p}{q}+2\right)}(x)$ satisfaisant $\beta>1+H(P)$ satisfait aussi

$$\beta\leqslant 1+\left(\frac{p}{q}+1\right)!pq^{\frac{p}{q}+1}H(P)^{\frac{p}{q}+2}\prod_{j=2}^{\frac{p}{q}+2}(jp-j+1)^2.$$

Ainsi , $f^{\left(\frac{p}{q}+1\right)}$ est croissante ou bien décroissante pour

$$x>1+\left(\frac{p}{q}+1\right)!pq^{\frac{p}{q}+1}H(P)^{\frac{p}{q}+2}\prod_{j=2}^{\frac{p}{q}+2}(jp-j+1)^2.$$

Supposons que $f^{\left(\frac{p}{q}+1\right)}$ décroissante. Elle est nécessairement strictement positive pour

$$x>1+\left(\frac{p}{q}+1\right)!pq^{\frac{p}{q}+1}H(P)^{\frac{p}{q}+2}\prod_{j=2}^{\frac{p}{q}+2}(jp-j+1)^2,$$

grâce à $\lim\limits_{x\longrightarrow\infty}f^{\left(\frac{p}{q}+1\right)}(x)=0$ par le Lemme 3.7.
En appliquant l'opérateur de différence Δ à f un nombre de fois égal à $\frac{p}{q}+1$, on trouve que $\left(\Delta^{\frac{p}{q}+1}f\right)(n)$ est un entier. On applique le théorème des valeurs intermédiares plusieurs fois pour obtenir un nombre $c_0\in(n,n+\frac{p}{q}+1)$ tel que $f^{\left(\frac{p}{q}+1\right)}(c_0)=\left(\Delta^{\frac{p}{q}+1}f\right)(n)$ est un entier.
Pour tout $k=1,\dots,M$, on repète le processus ci-dessus pour chaque bloc d'entiers consécutifs n_k+i, $i=0,\dots,\frac{p}{q}+1$, afin obtenir les nombres c_k tel que $c_k\in(n_k,n_k+\frac{p}{q}+1)$ et $f^{\left(\frac{p}{q}+1\right)}(c_k)=\left(\Delta^{\frac{p}{q}+1}f\right)(n_k)$ sont des entiers.

Par le lemme 3.10, l'entier $f^{\left(\frac{p}{q}+1\right)}(c_0) = \left(\Delta^{\frac{p}{q}+1} f\right)(n)$ est tel que

$$\begin{aligned}\left|f^{(\frac{p}{q}+1)}(c_0)\right| &= \left|\sum_{i=0}^{\frac{p}{q}+1} \binom{\frac{p}{q}+1}{i} (-1)^i f(n+\frac{p}{q}+1-i)\right| \\ &\leqslant \sum_{i=0}^{\frac{p}{q}+1} \binom{\frac{p}{q}+1}{i} |m_{\frac{p}{q}+1-i}| \\ &\leqslant M.\end{aligned}$$

Comme $f^{\left(\frac{p}{q}+1\right)}$ est décroissante, $f^{(\frac{p}{q}+1)}(c_k) < f^{(\frac{p}{q}+1)}(c_{k-1})$ pour tout $k = 1, ..., M$. D'où $f^{(\frac{p}{q}+1)}(c_j) \leqslant M - j$ pour $j = 0, ..., M$. Ceci entraine $f^{(\frac{p}{q}+1)}(c_M) \leqslant 0$, ce qui contredit le fait que $f^{(\frac{p}{q}+1)}(x)$ est strictement positive aux points $c_0, c_1, ..., c_M$, finalement, on obtient

$$c_M > c_0 > n > 1 + (\frac{p}{q}+1)! p q^{\frac{p}{q}+1} H(P)^{\frac{p}{q}+2} \prod_{j=2}^{\frac{p}{q}+2} (jp - j + 1)^2.$$

De la même manière , le cas où $f^{(\frac{p}{q}+1)}$ est croissante mène à une contradiction. Par suite, $f(x)$ est un polynôme et $P(x) = f(x)^q$. Ce qui achève la preuve du théorème. □

Conclusion

"*Et toute science, quand nous l'entendons non comme un instrument de pouvoir et de domination, mais comme aventure de connaissance de notre espèce à travers les âges, n'est autre chose que cette harmonie, plus ou moins vaste et plus ou moins riche d'une époque à l'autre, qui se déploie au cours des générations et des siècles, par le délicat contrepoint de tous les thèmes apparus tour à tour, comme appelés du néant*"

Alexander Grothendieck (Récoltes et semailles [15])

Dans ce travail, nous avons d'abord étudié des congruences modulo une puissance d'un nombre premier p concernant des coefficients binomiaux. Il s'agit essentiellement des congruences de Wolstenholme pour $\binom{2p-1}{p-1}$ et de Morley pour $\binom{p-1}{\frac{p-1}{2}}$. Nous avons étudié les améliorations successives de ces congruences obtenues par différents auteurs et par différentes méthodes jusqu'à nos jours. La plus récente avancée étant celle obtenue par Rosen qui a pu donner une méthode pour obtenir des super-congruences optimales pour le coefficient binomial $\binom{2p-1}{p-1}$. Nous avons pu apporter une contribution à cette étude en démontrant une congruence modulo p^7 pour le coefficient binomial $\binom{\alpha p-1}{p-1}$, α étant un p-entier. Ce résultat généralise à la fois la congruence de Wolstenholme (pour $\alpha = 2$) et la congruence de Morley (pour $\alpha = \frac{1}{2}$) et aussi, et surtout, ce résultat généralise et améliore des congruences pour les coefficients binomiaux $\binom{2p-1}{p-1}$ et $\binom{p-1}{\frac{p-1}{2}}$ obtenues par d'autres auteurs. Nous avons d'autre part analysé minutieusement les travaux de Keskin, Karaatli et Siar concernant l'étude très dense et approfondie des équations diophantiennes

$$x^2 - kxy + y^2 + 2^n = 0. \tag{3.1}$$

et

$$x^2 - kxy + y^2 - 2^n = 0. \tag{3.2}$$

réalisées par ces auteurs en 2012 [22] et 2013 [23].Cette analyse nous a permis de constater que l'étude réalisée par ces auteurs pourrait être encore complétée, prolongée ou encore être appliquée à d'autres équations diophantiennes. Ainsi nous avons pu répondre positivement à une conjecture concernant l'équation diophantienne (3.2) posée par ces auteurs dans [23] en prouvant non seulement que cette conjecture est vraie mais aussi en établissant un résultat analogue pour l'équation diophantienne (3.1).

Enfin, nous avons aussi étudié les polynômes dont les images des entiers sont des puissances d'entiers en donnant un théorème qui limite l'étude à un nombre fini de blocs de points consécutifs en améliorant partiellement un résultat de Shapiro sur les polynômes à valeurs entières.

Les outils développés pour étudier, comprendre et améliorer les congruences de Wolstenholme et de Morley et pour prouver la conjecture de Keskin, Karaatli et Siar ainsi que les polynômes à valeurs entières nous laissent entrevoir la possibilité de résoudre d'autres problèmes analogues.

Bibliographie

[1] M. Ayad and O. Kihel, Recognizing the primes using permutations, International Journal of Number Theory, 2012.

[2] C. Babbage, Demonstration of a theorem relating to prime numbers, Edinburgh Philosophical J. 1 (1819), 46–49.

[3] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Cambridge Philos. Soc.*, **65** (1969), 439-444.

[4] F. Bencherif, R. Boumahdi, and T. Garici, Generalization of Wolstenholme's and Morley's congruences, Pub. Math. Debrecen, Vol 93, 2018 to appear.

[5] R. Boumahdi and J. Larone, Polynomials with values which are powers of integers, Arch. Math. (Brno), accepted.

[6] R. Boumahdi, O. Kihel and S. Mavecha, Proof of the Conjecture of Keskin, Siar and Karaatli, Ann. Acad. Sci. Fenn. Math, vol 43, 2018, 557-561.

[7] E. Brown, Regiomontanus : His Life and Work (Amsterdam, 1990).

[8] L. Carlitz, A Theorem of Glaisher, Canadian Journal of Mathematics **5** (1953) :306-316

[9] L. Carlitz, Note on a Theorem of Glaisher. Journal of the London Mathematical Society. **28** (1953) : 245-246.

[10] W. H. J. Fuchs, A polynomial the square of another polynomial, *Amer. Math. Monthly*, **57** (1950), 114-116.

[11] C. F. Gauss,"Recherches arithmétiques, traduction française de Disquisitiones Arithmeticae." Blanchard, Paris (1953).

[12] J. W. L. Glaisher, Congruences relating to the sums of products of the first n numbers and to other sums of products, Q. J. Math. 31 (1900), 1–35.

[13] J. W. L. Glaisher, On the residues of the sums of products of the first $p-1$ numbers, and their powers, to modulus p^2 or p^3, Q. J. Math. 31 (1900), 321–353.

[14] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics (Addison-Wesley, 1994).

[15] A. Grothendieck, Récoltes et semailles, https ://www.quarante-deux.org/archives/klein/prefaces/.../Recoltes_et_semailles.pdf.

[16] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Clarendon, Oxford, 1980.

[17] S. Hawking, Et Dieu créa les nombres. Les plus grands textes de mathématiques réunis et commentés." Dunod (2006).

[18] Y. Hu and M. Le, On the Diophantine equation $x^2 - kxy + y^2 + \ell x = 0$, Chin. Ann. Math 34B (5),715-718, 2013.

[19] C. G. Ji, A simple proof of a curious congruence by Zhao, Proc. Amer. Math. Soc., 133(2005) : 3469-3472.

[20] J. P. Jones, Representation of solutions of Pell equations using Lucas sequences. Acta Acad. Paedagog. Agriensis, Sect. Mat. (N.S.) 30 (2003), 75–86.

[21] R. Keskin, *Solutions of some quadratic Diophantine equations*, Comput. Math. Appl., **60** (2010), 2225–2230.

[22] R. Keskin, O. Karaatlı, and Z. Şiar, *On the Diophantine Equation* $x^2 - kxy + y^2 + 2^n = 0$, Miskolc Math. Notes, **13** (2012), 375-388.

[23] R. Keskin, Z. Şiar and O. Karaatlı, *On the Diophantine Equation* $x^2 - kxy + y^2 - 2^n = 0$, Czechoslovak Mathematical Journal, **63** (138)(2013), 783-797.

[24] T. Kojima, Note on number-theoretical properties of algebraic functions, *Tohoku Math. J.*, **8** (1915), 24-27.

[25] J. C. Lagarias, On the computational complexity of determining the solvability or unsolvability of the equation $X^2 - DY^2 = -1$, Trans. Amer. Math.Soc. 260 (1980), 485–508.

[26] H. W. Lenstra Jr, Solving the Pell equation, Notices of the AMS, Volume 49 (2) (2002), 182-192

[27] H. A. Lenstra, Algorithmic Number Theory MSRI Publications, Volume 44, 2008.

[28] W. J. LeVeque, On the equation $y^m = f(x)$, *Acta. Arith.* **IX** (1964), 209-219.

[29] W. L. McDaniel, Diophantine representation of Lucas sequences. Fibonacci Q. 33 (1995), 59–63.

[30] R. J. McIntosh, On the converse of Wolstenholme's Theorem, Acta Arith. 71 (1995), 381–389.

[31] A. Marlewski and P. Zarzycki, *Infinitely many solutions of the Diophantine equation* $x^2 - kxy + y^2 + x = 0$, Comput. Math. Appl., **47** (2004), 115–121.

[32] D. W. Masser, Polynomial bounds for Diophantine equations, *Amer. Math. Monthly*, **93** (1980), 486-488.

[33] Y. Matiyasevitch, Le dixième problème de Hilbert : son indécidabilité, édition Masson, 1995.

[34] R. Melham, Conics which characterize certain Lucas sequences. Fibonacci Q. 35 (1997), 248–251.

[35] R. Meštrović, An extension of Babbage's criterion for primality, Math. Slovaca 63, no. 6 (2013), 1179–1182.

[36] R. Meštrović, On the mod p^7 determination of $\binom{2p-1}{p-1}$, Rocky Mountain Journal of Mathematics, 44 (2), (2014), 633-648.

[37] R. A. Mollin, Simple continued fraction solutions for Diophantine equations, Expositiones Mathematicae, 19(2001), 55-73.

[38] R. Mollin, and A. Srinivasan A note on the Pell negative equation, Int J of Algebra,Vol 4 (2010), n19, 919-922.

[39] F. Morley, Note on the congruence $2^{4n} \equiv (-)^n (2n)!/(n!)^2$, where $2n+1$ is a prime, Ann. of Math. 9 (1894/95), no. 1-6, 168–170.

[40] T. Nagell, *Introduction to number theory*, John Wiley & Sons, Inc., New York, Stockholm, 1951.

[41] C. Pascal. Histoire des sciences arabes, sous la direction de Roshdi Rashed avec la collaboration de Régis Morelon. Revue du monde musulman et de la Méditerranée, 83(1), (1997) 219-223.

[42] D. Poulakis, A simple method for solving the Diophantine equation $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, *Elem. Math.*, **54(1)** (1999), 32-36

[43] M. Rolle, *Traité d'algèbre*, Paris, 1690.

[44] J. Rosen, Multiple harmonic sums and Wolstenholme's theorem, Int .J. Number Theory, 9(8), 2013, 2033-2052.

[45] J. H. Rosen, The Arithmetic of Multiple Harmonic Sums (Doctoral dissertation, University of Michigan) (2013).

[46] H. S. Shapiro, The range of an integer-valued polynomial, *Amer. Math. Monthly*, **64** (1957), 424-425

[47] N. J. Sloane et al, *The on-line Encyclopedia of Integer Sequences.*URL https ://oeis.org/, [*Online*], 2017.

[48] L. Szalay, Superelliptic equations of the form $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \cdots + a_0$, *Bull. Greek Math. Soc.*, **46** (2002), 23-33.

[49] R. Tauraso, More congruences for central binomial coefficients, J. Number Theory **130** (2010), 2639–2649.

[50] S. Tengely, Effective methods for Diophantine equations., Ph.D. thesis, Thomas Stieltjes Institute for Mathematics, 2005.

[51] A. Thue. Uber Annaherungswerte algebraischer Zahlen. J. reine angew. Math.,135 :284-305, 1909.

[52] R. Tijdeman, On the equation of Catalan, *Acta Arith.*, **29(2)** (1976), 197-209.

[53] P. M. Voutier, An upper bound for the size of integral solutions to $Y^m = f(X)$, *J. Number Theory*, **53** (1995), 247-271.

[54] P. G. Walsh, A quantitative version of Runge's theorem on Diophantine equations, *Acta Arith.*, **62(2)** (1992), 157-172.

[55] J. Wolstenholme, On certain properties of prime numbers, Quart J. Math. **5** (1862) 35-39.

[56] S. Y . Yan, Number theory for computing., Berlin : Springer, 2000.

[57] P. Yuan and Y. Hu, *On the Diophantine equation* $x^2 - kxy + y^2 + \ell x = 0$, $\ell \in \{1, 2, 4\}$, Comput. Math. Appl., **61** (2011), 573–577.

[58] J. Zhao, Bernoulli Numbers, Wolstenholme's theorem, and p^5 variations of Lucas' theorem, J. Number Theory 123 (2007), 18–26.