Université Cheikh Anta Diop de Dakar

École Doctorale Mathématiques et Informatique

N^o d'ordre: **XXXX**

THÈSE DE DOCTORAT UNIQUE

Mention: *Mathématiques et Modélisation*
Spécialité: *Codage, Cryptologie, Algèbre et Applications*

Présenté par

Aboussaghid Alkabouss Sakha

Pour obtenir le grade de
Docteur de l'Université Cheikh Anta Diop de Dakar

Titre: Équations Diophantiennes: Formes Quadratiques et Nombres de Classes

Soutenue le 11 Mars 2019 devant le jury composé de:

Président:	Mamadou SANGHARÉ	Professeur	Univ. Cheikh Anta Diop
Rapporteurs:	Farid BENCHERIF	Professeur	Univ. des Sciences et Technolo Houari Boumediene, Algérie
	Kacem BELGHABA	Professeur	Univ. Oran I, Algérie
Examinateurs:	Oumar DIANKHA	Professeur	Univ. Cheikh Anta Diop
	Ismaïla DIOUF	Maître de Conférences (CAMES)	Univ. Cheikh Anta Diop
	Abdoul Aziz CISS	Maître Assistant (CAMES)	Ecole Polytechnique de Thiès
Directeurs de thèse:	Omar KIHEL	Professeur	Brock University, Canada
	Djiby SOW	Professeur	Univ. Cheikh Anta Diop

Dédicaces

Je dédie ce modeste travail :

A ALLAH LE TOUT PUISANT.

A mes chers et tendres parents,

A mes chers grand parents,

A mes frères et sœurs,

A mes oncles et tantes,

A mes neveux et nièces,

A mes cousins et cousines,

A tous mes amis,

A tous mes enseignants,

A toutes les personnes qui ont contribué de prés ou de loin à ma formation.

Remerciements

Au nom d'ALLAH, le tout miséricordieux le très miséricordieux.
Qu'Allah soit loué et que la paix et le salut soit sur le prophète Mohamed.

Je voudrais tout d'abord adresser mes sincères remerciements à Monsieur le Professeur **Mamamadou Sangharé** pour l'honneur qu'il m'a fait de présider mon jury de thèse.

Je tiens à exprimer mes plus chaleureux remerciements à mon directeur de thèse le Professeur **Omar Kihel**. Je vous suis reconnaissant pour avoir guidé mes premiers pas dans le monde de la recherche et pour vos précieux conseils. J'ai apprécié votre sens d'écoute au cours de nos interminables discussions. Votre rigueur scientifique, votre générosité et votre ouverture d'esprit m'ont marqué à vie.

Je voudrais remercier particulièrement mon co-directeur de thèse le Professeur **Djiby Sow**. J'ai beaucoup apprécié votre franchise, votre simplicité et votre disponibilité pour mes abondantes questions. Je vous suis reconnaissant pour les enseignements que j'ai reçu de vous que ça soit du point de vue scientifique et humain.

Je tiens à remercier vivement Messieurs les professeurs **Farid Bencherif** et **Kacem Belghaba** pour avoir accepté de rapporter cette thèse.

Je souhaite exprimer toute ma reconnaissance aux Pr **Oumar Diankha**, Pr **Ismaïla Diouf** et Dr **Abdoul Aziz Ciss** pour l'honneur qu'ils m'ont fait de siéger dans mon jury de thèse en tant que examinateurs.

Je remercie sincèrement Dr Abdoul Aziz Ciss, sa femme Aminata Diallo ainsi que toute

sa famille de m'avoir accueilli chez lui et de me considérer comme son propre frère. Je ne le remercierai jamais assez.

J'aimerais exprimer ma profonde gratitude au Pôle de Recherche en Mathématiques et leurs Applications à la Sécurité de l'Information **(PRMASI)** financé par la Fondation Simons pour leur soutien financier sans lequel cette thèse n'aura pas eu lieu. Je remercie tous les membres du projet, en particulier, la facilitatrice Pr Marie Françoise Roy, Pr Djiby Sow, Dr Tony Ezome, Dr Abdoul Aziz Ciss, Dr Emmanuel Fouotsa.

Je tiens à remercier mes collaborateurs scientifiques pour leurs suggestions et leurs disponibilités : Pr Benseba Boualem, Dr Tariq Garici, Jesse Larone et Nacera Berbara.

Je souhaite remercier tous les membres de notre équipe de recherche **ASCSI** dirigé par le Pr Djiby Sow. Dr Abdoul Aziz Ciss, Dr Demba Sow, Dr Mame Demba Cissé, Dr Nafissatou Diarra, Dr Bernadette Faye Fall, Dr Ousmane Ndiaye, Dr El hadji Demba Wade Diop, Dr J. Raoul Tsiba, Dr Mamadou G. Camara, Dr Landing Fall, Dr Ahmed Youssef, Dr Lamine Ngom, Dr Hortense Boudjou Hardy, Bernard Ousmane Sané, Soda Diop Fall, Moussa Sall, Jean-Louis Tabar, Mamamdou Lamine Diallo, Babacar Ndiaye, Pape Modou Ndiaye, Moussa Diedhou. Je remercie particulièrement Moustapha Seck (Michel), Abdoulaye Mbaye, Abdoulaye Maiga, Mamadou Sall, Mobouale Wamba Stonn, Yatma Diop. Merci pour tous ces moments inoubliables passés ensemble, pour vos questions instructifs, vos conseils, vos suggestions, vos remarques,.... pendant les séminaires.

Mes remerciements vont également aux membres du département Génie Informatique et Télécommunication de l'Ecole Polytechnique de Thiès, je nomme Pr Oumar Niang, Dr Abdoul aziz Ciss, Dr Abdoulaye Guissé, Dr Ndeye Fatou Ngom, Mme Sy, Dr Diallo Diouf, Dr Ibrahima Gueye, Dr Samba Sidibé, Dr Ahmad Wade pour m'avoir offert un cadre de travail idéal. Je remercie spécialement Cheikh Mohamed Guera mon compagnon du bureau pour tes conseils et ta curiosité mathématique. Je profite pour remercier Pr Mamadou Wade pour l'opportunité qu'il m'a offerte de loger à l'EPT pour les trois derniers mois de mon séjours à Thiès.

Je désire exprimer toute ma gratitude à : l'association Grain de Sable pour son soutien pendant le lycée ; mes tuteurs pendant le collège que sont Ahmad Allo, sa femme Hadjia Haoua Boubacar et Ahmad Hammo ; Mr Assalih Jaghfar et sa femme Assalama Mahmoud pour leur hospitalité et leur gentillesse pendant mes premiers mois au Sénégal. Un grand merci également à tous les membres du Foyer des Étudiants de Timia.

Un grand merci à tous les doctorants de l'EPT, Spécialement à Dr Salif Diallo, Dr C.T Cherif Ndiaye, Abdoul Dalibou Abdou et à tous les doctorants de l'UCAD, pour les moments partagés pendant les séminaires des doctorants. Je remercie également les étudiants nigériens de Thiès.

Merci à tous mes amis et camarades du Niger au Sénégal en passant par l'Algérie : Nouhan Issouffa, Sidi Agalher, Ghabdoullah Alkabouss, Adouma Alghoubas, Sidi Aghali, Mohamed Idrissa, Harouna Ahmadou, Malik Assalih, Oussamatou Abdou Mainassara, Dr Ibrahim Souleymane Arzika, Djibrilla Moussa Bonkano, Ismael Aboubacar Tondi, Abdoulrazak Sani Balla, Stefanous Ado, Hamid Benjelida, Seddik Mohamed, Hannaa Moukadem, Fouzia Belmokadem, Pape Birame Sye, Gilbert Dione, Ousmane Ouadragou,.....

Je voudrais remercier tout le personnel administratif du département de Mathématiques-Informatique de l'UCAD, en particulier au chef du département Pr Mamadou Barry, à mon ami Mr. Boubacar Sow, à Mme Bâ, à Mme Mbaye, à Mr Massaly.

Un grand merci à mes étudiants de licence 3 TDSI option Maths-Crypto-Sécurité et mes étudiants L1 PCSM. Merci pour vos questions.

Enfin, je garde ces derniers mots pour exprimer toute ma reconnaissance à toute ma famille, pour leur encouragement, leur soutien moral, leurs conseils, bref pour tous.

je souhaite remercier toutes les personnes que j'ai oubliées de mentionner, je m'en excuse sincèrement.

Table des matières

Résumé

L'analyse diophantienne est la branche de la théorie des nombres qui traite, en particulier, les équations polynomiales à coefficients entiers et dont les solutions recherchées sont entières. Ce genres d'équations sont appelées équations diophantiennes. Le manque d'une méthode générale pour résoudre une équation diophantienne quelconque ouvre la voie à la mise en place des méthodes spécifiques. Pour certaines familles d'équations diophantiennes ces méthodes spécifiques existent.
Dans cette thèse, nous avons apporté les contributions suivantes.
Soient $Res_x(P(x), Q(x))$ le résultant en x de deux polynômes, s, t et a des entiers rationnels. En utilisant une amélioration de la méthode de Runge due à Schinzel, nous avons démontré que l'équation diophantienne de type résultant, donnée par

$$Res_x(P(x), x^2 + sx + t) = a$$

admet un nombre fini de solutions entières.
Nous avons étudié aussi l'équation diophantienne $x^2 - kxy + ky^2 + ly = 0$ où k et l sont des entiers avec k pair. Nous avons également considéré la même équation quand $l = 3^n$ et $k \equiv 2$ (modulo 3) ; $l = 2^r 3^s$ et $k = 2k' + 1$ avec $k' \equiv 2$ (modulo 3) où n, r et s sont des entiers positifs. Nous avons utilisé la théorie des équations de Pell-Fermat généralisées pour fournir une caractérisation des solutions entières de ces équations.
Enfin, nous avons obtenu une borne inférieure sur les $h+1$ plus petits nombres premiers qui se décomposent dans un corps quadratique imaginaire où h désigne le nombre des classes de ce corps.

Chapitre 1

Introduction générale

Dans cette thèse, nous serons concernés par trois problèmes différents de l'analyse diophantienne, domaine de la théorie des nombres qui traite, en particulier, des solutions entières des équations algébriques. Une équation diophantienne est une équation polynomiale à coefficients entiers dont les solutions sont recherchées parmi les entiers relatifs ou, éventuellement, les nombres rationnels. Autrement dit, c'est une équation de la sorte

$$f(x_1, x_2, ..., x_n) = 0,\ f \in \mathbb{Z}[X_1, ..., X_n]$$

où les $x_1, ..., x_n \in \mathbb{Z}$ ou $\mathbb{Q}$. Il arrive que l'on considère aussi des solutions dans des corps de nombres ainsi que dans leurs anneaux d'entier. Nous remarquons que si l'équation est à coefficients rationnels, alors en la multipliant par le plus petit multiple commun de ses coefficients nous retrouvons une équation à coefficients entiers, ce qui justifie la restriction aux coefficients entiers dans la définition ci dessus.

Généralement, quand on étudie une équation diophantienne trois questions se posent naturellement :

1-a) L'équation admet-elle de solutions entières ?
1-b) L'équation admet-elle de solutions rationnelles ?
2) Les solutions sont elles en nombre fini ou infini ?
3) Peut-on obtenir toutes les solutions ?

Dans le cas homogène les solutions entières déterminent les solutions rationnelles,

c'est à dire rechercher les solutions entières revient à rechercher les solutions rationnelles, et vice versa. Par contre dans le cas non homogène, les questions traitant les solutions entières sont beaucoup plus difficiles que celles traitant les solutions rationnelles.

Dans certains cas particuliers, une réponse affirmative à ces questions est possible, concourant les travaux de plusieurs mathématiciens parfois sur plusieurs siècles. En générale, on n'est même pas capable de répondre à la première question. En effet, dans sa fameuse liste de 23 problèmes énoncés lors du congrès international de mathématiques à Paris en 1900, David Hilbert proposa en guise du dixième problème de trouver un algorithme qui permet de décider si une équation diophantienne générale est résoluble. Autrement dit, le problème propose de trouver une méthode générale qui étant donné une équation diophantienne quelconque décide s'il existe des entiers $x_1, x_2, ..., x_n$ tels que $f(x_1, x_2, ..., x_n) = 0$. En 1970, Y. Matiyasevich montra que les ensembles diophantiens sont récursivement énumérables, parachevant les travaux de logiciens J. Robinson, M. Davis, H. Putnam. Comme conséquence de son résultat, l'algorithme que demandait Hilbert ne peut exister. Toutefois, pour certaines familles particulières des équations diophantiennes un tel algorithme existe. L'analogue du dixième problème de Hilbert pour les solutions rationnelles n'est pas encore résolue, notamment de trouver un algorithme qui décide s'il existe des rationnels $x_1, x_2, ..., x_n$ tels que $f(x_1, x_2, ..., x_n) = 0$.

Pour placer dans le contexte adéquat nos contributions, il nous semble nécessaire de faire un bref historique de ladite théorie.
La théorie des nombres est l'un des domaines les plus anciens et les plus fondamentaux des mathématiques, puisque la nature et les propriétés des nombres entiers ont toujours fasciné les hommes. Il convient de mentionner aussi que c'est un domaine de recherche très actif, où on y rencontre plus des problèmes ouverts que dans n'importe quel autre domaine de mathématiques et des nombreux auteurs s'y intéressent. De ce point vue le mathématicien E. T. Bell disait de la théorie de nombres : *"Le dernier grand continent non civilisé de mathématiques."*

Des découvertes récentes ont montré que la civilisation Mésopotamienne est la plus

ancienne dont nous possédons une trace de l'activité mathématique, plus particuliérement de l'analyse diophantienne. En effet, on trouve dans une tablette en argile en écriture cunéiforme, connue sous le nom du Plimpton 322 (conservée à la bibliothèque Plimpton de l'université de Columbia de New York) publiée par O. Neugebauer et A. Sach en 1945 (voir [58]). Cette tablette est datable de l'époque de la première dynastie babylonienne et contient une liste des triplets pythagoriciens, c'est à dire des entiers x, y, z tels que $x^2 + y^2 = z^2$. L'analyse de cette tablette montre que les anciens babyloniens possédaient une méthode générale pour résoudre en entier l'équation de Pythagore. Il faut signaler aussi que les anciens égyptiens, les indiens et les chinois ont aussi étudié certaines propriétés de nombre entiers. Dans la la Grèce antique débuta la mathématique en général, telle que nous la connaissons aujourd'hui (théorème, preuve, déduction, etc). Euclide d'Alexandrie, une figure mathématique emblématique de la Grèce antique, synthétisa les résultats mathématiques connus de l'époque dans son livre : les Eléments. Les livres VII, VIII et IX des éléments d'Euclide sont dédiés à la théorie des nombres. On y trouve par exemple, l'une des plus belles démonstrations de l'histoire de mathématiques, notamment, l'existence d'une infinité de nombre premiers ; un procédé de calcul de plus grand commun diviseur de deux nombres, connu de nos jours sous le nom d'algorithme euclidien et aussi un critère sur le nombre parfait, qui est jusqu'aujourd'hui le meilleur résultat de ce genre, pour ne citer que ceux là.

Les équations diophantiennes sont nommées en l'honneur du mathématicien grec Diophante d'Alexandrie. Diophante a rédigé un traité composé de treize volumes du livre intitulé Arithmétique, dont seulement six en texte grec ont survécu. Diophante dans son arithmétique se contentait seulement d'une seule solution rationnelle positive aux équations algébriques à coefficient entiers même si l'équation admet une infinité de solutions. Il était le premier à introduire le symbolisme algébrique bien que limité. En effet, il possédait l'abréviation pour une seule inconnue et les puissances positives ou négatives de cette dernière. D'un point de vue moderne, la plus part des problèmes que considérait Diophante revient à la recherche des points à coordonnées rationnelles sur les courbes algébriques de genre 0 ou 1. Comme exemple,on peut citer, le cas d'une conique plane $y^2 = ax^2 + bx + c$ où a ou c sont de carrés. Diophante considérait aussi des problèmes d'autre genre. Par exemple, le problème de trouver

trois nombres rationnels dont le produit de chaque deux d'entre eux augmenté au troisième est un carré. Un autre problème demande de trouver un ensemble de quatre nombre rationnels tels que le produit de chacun des deux additionné à un est un carré, ce genre d'ensemble porte de nos jours le nom de quadruplet diophantien. Un dernier exemple que nous voulons citer est le problème 19 du livre III, tiré de Houzel [38], qui questionne de trouver quatre nombres rationnels tels que le carré de leur somme additionné ou soustrait de chacun d'eux est un carré.

En Inde, l'astronome et mathématicien Aryabhata, qui a vécu au sixième siècle, proposait une méthode générale pour la résolution en entier de l'équation diophantienne linéaire, autrement du type $ax + by = c$ pour des besoins d'astronomie, Diophante ne considérait que des équations de degré supérieur, car le cas linéaire est évident pour les solutions rationnelles. Cette méthode a été reprise par ses successeurs, tels que Brahmagupta (VII^e siécle), qui lui donnaient le nom de kuṭṭaka, qu'on peut traduire par "pulvérisateur" d'après A. Weil [79]. Brahmagupta traita aussi quelques cas de l'équation dite maintenant de Pell-Fermat, donnée par l'équation

$$x^2 - dy^2 = m$$

où d est un entier positif sans facteur carré, $m \in \{\pm 1, \pm 2, \pm 4\}$ et x et y sont recherchés parmi les entiers. Il a introduit une identité dite bhāvanā qui s'apparente à une loi de composition, car elle permet, étant donné une solution, d'obtenir une autre. Bhāskara (XII^e siécle) donna une solution générale de la même équation via une méthode cyclique, dite cakravāla.

L'apport des mathématiciens arabo-musulmans du X^e siècle en analyse diophantienne réside, en gros, dans l'adaptation du système de numération indien et la conservation de connaissances de civilisations précédentes tels que les grecs et les indiens. Néanmoins, leurs contributions sont plus importantes dans la nouvelle algèbre (mot qui vient d'ailleurs de l'arabe) et en trigonométrie. Dans la lignée du problème 19 du livre III de Diophante, cité ci-dessus, Al-khāzin posa le problème du nombre congruent, qui n'est toujours pas totalement résolu. Plus précisément, il proposa de trouver les nombres n tels que $x^2 - n$ et $x^2 + n$ soient des carrés. Autrement dit, de trouver des

nombres qui sont la différence commune d'une progression arithmétique de carrés rationnels à trois termes. A cause de l'égalité $c^2 \pm 2ab = (a \pm b)^2$ pour un triplet pythagoricien , il démontre qu'un tel nombre serait le quadruple de l'aire d'un triangle rectangle rationnel. D'un point de vue moderne, un nombre est congruent s'il est l'aire d'un triangle rectangle à côtés rationnels. Ce problème est équivalent aussi à déterminer si la courbe elliptique définie par l'équation $y^2 = x^3 - n^2 x$ a un rang positif ou qu'elle possède un point rationnel (x, y) avec $y \neq 0$.

Leonardo Fibonnacci, aussi connu sous le nom de Léonard de Pise (vers fin du douzième siècle et vers la moitié du treizième siècle), était le premier à introduire le système de numération arabo-indien en Europe. En effet, c'est un grand voyageur qui a vécu en Afrique du nord et s'est familiarisé avec les mathématiques arabes. Il a repris le problème de nombre congruent d'Al-khāzin, dans son livre des nombres carrés (1225) et démontra l'identité algébrique

$$(x^2 + y^2)(u^2 + v^2) = (xv \pm yu)^2 + (xu \mp yv)^2$$

déjà explicitée par Al-khāzin et présente implicitement dans les travaux de Diophante. Il démontra que si x est un entier alors n est un multiple de 24 et que 5 et 7 sont congruents. Il est plus connu par la suite d'entiers positifs, qui porte maintenant son nom, dont les termes initiaux sont 0 et 1 et le terme suivant est la somme de deux termes précédents. Il y a dans la littérature beaucoup de résultats sur les équations diophantiennes qui utilisent la suite de Fibonacci.

En Europe, Regiomontanus (15^{eme} siècle) était le premier à redécouvrir le traité de Diophante. R. Bombelli (16^{eme} siècle) l'a redécouvert à la bibliothèque du Vatican et a inséré une grande partie du manuscrit de Diophante dans son algèbre de 1572. La première traduction en latin de l'arithmétique de Diophante est l'œuvre de G. Xylander, en 1575, accompagné de certains commentaires. François Viète a inséré aussi une grande partie de l'arithmétique de Diophante dans son Zetetica de 1593. Il était le premier à introduire la notation par des lettres les coefficients des équations algébriques en suivant l'idée de Diophante pour l'inconnue. Dans sa reprise de Diophante, Viéte est beaucoup plus intéressé par l'algèbre et la trigonométrie que la théorie de nombre et

de mettre en valeur ses propres découvertes. La traduction de Diophante par Xylander est défectueuse et contient de nombreuses coquilles. En 1621 Bachet de Méziriac publia le manuscrit en grec de Diophante accompagné d'une traduction en latin meilleur que celle de Xylander et de nombreux commentaires. Bachet a repris l'équation diophantien linéaire, sans être au courant de son traitement par les mathématiciens indiens mentionné ci dessus, qu'il a résolu complètement dans la deuxième édition de ses Problèmes plaisants et délectables de 1624. Il remarqua aussi que dans certains problèmes, Diophante assume que tout entier est la somme d'au plus quatre carrés et il a essayé d'en apporter une preuve sans succès. Ce problème sera repris par ses successeurs. Bachet considéra aussi le problème d'écrire un entier comme la différence d'un carré et d'un cube qui revient à résoudre l'équation diophantienne $y^2 - x^3 = m$ avec m un entier relatif. Cette équation porte le nom du mathématicien anglais L. J. Mordell qui l'a étudiée profondément au 20^{eme} siècle.

Pierre de Fermat (1601-1665) est considéré comme étant le fondateur de la théorie de nombre moderne. Il avait étudié attentivement et profondément l'édition de Bachet de l'arithmétique de Diophante et il y a annoté ses découvertes sur les marges. Durant sa lecture sur la partie concernant les triplets pythagoriciens, Fermat énonça ceci : *"Il est impossible de décomposer un cube en deux cubes, un bicarré en deux bicarrés et plus généralement une puissance n-ième plus grande que* 2 *en deux puissances de même degré* et il ajoute : *J'ai découvert une preuve remarquablement merveilleuse dont cette marge est trop étroite à contenir*. Sa preuve n'a jamais été retrouvée et il subsiste des doutes sur son existence. Cet énoncé qui était connu sous le nom du **dernier théorème de Fermat** (bien que ce n'était pas un théorème) peut être reformulé comme suit : *Il n'existe pas des entiers rationnels x, y et z strictement positifs tels que*

$$x^n + y^n = z^n$$

avec $n > 2$. Fermat avait introduit sa méthode de descente infinie, dont le principe repose sur le fait qu'il n'existe pas une suite d'entier positif infinie strictement décroissante, pour démontrer que l'équation diophantienne $x^4 + y^4 = z^2$ n'admet pas de solutions entières et c'est la seule démonstration connue de Fermat. Ce résultat admet deux conséquences. La première est que son dernier théorème est vrai pour l'exposant

$n = 4$. La deuxième conséquence est la preuve que l'aire d'un triangle rectangle à côtés rationnels ne peut être un carré, ce qui implique que 1 n'est pas congruent, ce qui revient à dire qu'un carré n'est pas un nombre congruent.
Fermat dit avoir démontré plusieurs autres résultats par descente infinie, comme entre autres son **théorème de deux carrés**, ainsi que des théorèmes sur la représentations des nombres par des équations diophantiennes quadratiques. Il faut dire qu'à cette époque, tout se fait par correspondance et par défi et que Fermat manquait d'interlocuteurs qui partagent la même passion que lui, qui est la théorie de nombres, malgré tout ses efforts. La théorie des nombres est considérée comme un sujet moins important par les contemporains de Fermat.
En 1657, Fermat lançait un défi au mathématiciens anglais, n'étant pas au courant des travaux de mathématiciens indiens du septième siècle, de résoudre en entier l'équation de Pell-Fermat $x^2 - ny^2 = 1$, n sans facteur carré fixé, outre que la solution triviale $x = 1$ et $y = 0$. W. Brouncker et J. Wallis ont relevé le défi bien qu'ils n'avaient pas démontré qu'une seule solution existe toujours, ce que Fermat savait par descente infinie.

Leonhard Euler(1707-1783) qui a découvert les travaux de Fermat par l'intermédiaire de son ami C. Goldbach a passé plus d'un demi siècle à essayer de démontrer les théorèmes de Fermat. Il démontra le dernier théorème de Fermat pour l'exposant $n = 3$, avec tout de même quelques trous.
Euler démontra, également, les théorèmes de Fermat sur la représentation de nombres premiers par dés équations quadratiques, par exemple **si p est un nombre premier impair alors**

$$p = x^2 + 2y^2, x, y \in \mathbb{Z} \Longleftrightarrow p \equiv 1, 3 (\text{mod } 8).$$

Il prouva et conjectura plusieurs problèmes de ce genre, qui préludent la théorie de formes quadratiques binaires. C'est durant des tentatives numériques sur ces problèmes qu'il conjectura la loi de réciprocité quadratique.
Euler a, aussi, contribué dans l'étude de l'équation de Pell-Fermat. C'est d'ailleurs lui qui l'a faussement attribué au mathématicien anglais J. Pell sans aucune justificative, car il n'avait jamais étudié l'équation en question. Euler, à travers une identité algébrique qui n'est autre que le Bhavana de Brahmagupta cité ci dessus, parvenait à obtenir une infinité de solutions à l'équation. Il utilisa les fractions continues dans l'étude

de cette équation.

Sur la lignée du dernier théorème de Fermat, Euler conjectura que pour tout entier positif $n > 2$ la somme de $n-1$ puissances $n^{ème}$ ne peuvent être une puissance $n^{ème}$. Cette conjecture a été réfutée en 1988 par N. Elkies qui montre, grâce à la théorie de courbes elliptiques et l'usage des ordinateurs, que

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Euler a prouvé aussi, que les seules carrés et cubes consécutifs sont 8 et 9, autrement les seules solutions positifs à l'équation

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

sont $x = 8$ et $y = 9$.

J. L. Lagrange (1736-1813) a démontré que le développement en fraction continue de tout irrationnel quadratique est périodique à partir d'un certain rang. Il obtient comme conséquence que l'équation de Pell-Fermat admet toujours une solution et que les solutions sont en nombre infini .

Lagrange a aussi traité le problème de représentation des entiers par des formes quadratiques binaires suivant Euler, en considérant les équations plus générales de la forme

$$ax^2 + bxy^2 + cy^2$$

et il en fait une étude systématique en introduisant les notions de discriminants, des substitutions linéaires, d'équivalences de formes, des formes quadratiques binaires réduites et de façon implicite la composition des formes dans ses *Recherches d'arithmétiques*.

Il démontra, également, en exploitant une idée d'Euler, le théorème de quatre carrés que Fermat disait en posséder une preuve.

A. M. Legendre(1752-1833) publia le premier livre de la théorie des nombres en 1798 sous le nom *Essai sur la théorie des nombres*. Il y incorpora les travaux d'Euler et La-

grange. Il a repris les travaux de Lagrange sur les formes quadratiques binaires en introduisant la composition de formes et la théorie du genre. Il a introduit, également, un caractère quadratique qui porte maintenant son nom. Il a fait une tentative de preuve infructueuse de la loi de réciprocité quadratique.
Legendre donna une condition nécessaire et suffisante, connue sous le nom du théorème de Legendre, pour que l'équation diophantienne de la forme

$$ax^2 + by^2 + cz^2 = 0$$

aient des solutions entières en x, y et z.

Avec C. F. Gauss(1777-1855), la théorie des nombres est devenue une branche mûre et structurée de la mathématique et non une collection des problèmes. Gauss publia en 1801 ses *Disquisitiones arithmeticae* [30] qui éclipse le livre de Legendre mentionné plus haut. Le mathématicien J. P. Serre disait, lors de son exposé à l'occasion de bicentenaire de E. Galois, que c'est *un livre fondateur* et que *la théorie des nombres a la chance d'avoir un livre parfaitement rédigé, en ce sens qu'il a servi de modèle.* Gauss a introduit l'arithmétique modulaire qui a facilité la résolution de plusieurs types équations diophantiennes.
Dans ses Disquisitiones, Gauss développa la théorie des formes quadratiques binaires dans toute sa généralité. Il énonça sa théorie de l'équivalence propre pour les formes, les formes réduites, les classes de formes ayant le même discriminant, la théorie de genres pour les formes. Il énonça plusieurs conjectures sur le nombre de classes de formes quadratiques dont d'autres sont toujours non résolues.
Gauss démontra la loi de réciprocité quadratique qui permet la résolution des nombreuses équations diophantiennes quadratiques, il en donnera plusieurs démonstrations et l'appelle *le théorème d'or.*

Depuis le $19^{ème}$ siècle la théorie des nombre s'est développée dans des nombreuses directions. En effet, la théorie s'est subdivisée en sous-domaines en fonction de méthodes utilisées pour la résolution de ses problèmes.
Quelques avancées sur le dernier théorème de Fermat ont été faite aussi. En effet, Dirichlet et Legendre (1825) ont résolu le cas $n = 5$, le cas $n = 14$ a été résolu par Dirichlet

(1832), Lamé (1839)a résolu le cas $n = 7$. Sophie Germain (1831) a montré le premier cas du théorème de Fermat, autrement dit quand $p \nmid xyz$, pour l'exposant premier p pour lequel $2p + 1$ est aussi premier. Kummer (1846), en utilisant la théorie des corps cyclotomiques, a démontré le théorème pour l'exposant premier p régulier (ne divisant pas le nombre des classes d'idéaux de l'anneau des entiers du corps en question)
Ces avancées ont été possible grâce à la théorie algébrique des nombres développée suite aux travaux de Gauss sur la théorie des formes quadratiques binaires par C. G. L. Dirichlet, C. J. Jacobi, E. Kummer, R. Dedekind.
Dirichlet (1837) a aussi introduit les méthodes analytiques dans la démonstration de son théorème de la progression arithmétique (imitant quelque peu Euler dans sa démonstration de l'existence d'un nombre infini des nombres premiers), c'est la naissance de la théorie analytique de nombres.

En 1844, E. C. Catalan conjectura que *"Deux nombres entiers consécutifs autre que* 8 *et* 9 *ne peuvent être des puissances exactes.* En d'autre terme, l'équation diophantienne

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

n'admet qu'une seule solution entière $x = 2,\ y = 3,\ m = 3$ et $n = 2$. Le cas particulier déjà traité par Euler cité plus haut.

Soit $f(x, y)$ un polynôme à coefficients entiers rationnels de degré n et irréductible dans le corps des nombres rationnels. Considérons l'équation diophantienne

$$f(x, y) = 0.$$

On dit que $f(x, y)$ vérifie la condition de Runge si sa partie homogène dominante, autrement dit la somme des monômes de degré n, n'est pas une puissance d'une forme irréductible à une constante multiplicative prés.
En 1887, C. Runge [64] a démontré le premier résultat général sur les solution entières d'une équation diophantienne à deux inconnues. Plus précisément, il a démontré le théorème suivant (en fait, le théorème que l'on donne est un cas particulier).

Théorème 1.0.1. *Si $f(x, y)$ ne vérifie pas la condition de Runge, alors l'équation $f(x, y) =$*

0 *admet une infinité des solutions entières.*

En 1901, H. Poincaré [63] a repris une idée géométrique de Newton qui consiste à ramener la détermination des solutions rationnelles de l'équation diophantienne $y^2 = f(x)$ avec $f(x)$ de degré 3 à celle des points rationnels (à coordonnées rationnelles) de la cubique plane définie par cette équation. Au moyen des transformations birationnelles et la paramétrisation des courbes de genre 1 par des fonctions elliptiques, il a démontré que toute courbe rationnelle de genre 1 et de degré $n > 3$, qui admet un point rationnel donné est équivalent, dans le sens où la courbe peut se ramener, à une courbe cubique (voir Mordell [56]).
Il a conjecturé, en plus, que l'ensemble des points rationnels d'une courbe algébrique de genre 1 (qui est appelée une courbe elliptique) définie sur le corps des rationnels est un groupe abélien de type fini.

A. Thue [75] a obtenu, en 1909, un autre résultat général dans l'étude des équations diophantiennes à deux inconnues. En effet, il montre que pour un polynôme homogène irréductible $f(x, y)$ à coefficients entiers de degré $n \geqslant 3$ et un entier rationnel m, l'équation

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

n'admet qu'un nombre fini de solutions entières.
Ce résultat, Thue l'a obtenue comme conséquence de son théorème d'approximation diophantienne, domaine de la théorie des nombres qui traite des approximations des réels par les nombres rationnels.

Mordell, parvient à résoudre la conjecture de Poincaré en 1922. Il a conjecturé que dans le cas de genre $g \geqslant 2$, l'ensemble des points rationnels est fini.
Siegel [70] a obtenu, en 1929, un résultat remarquable similaire à la conjecture de Mordell dans le cas des points entiers. En effet, Il a montré que toute courbe algébrique irréductible de genre $g \geqslant 1$ n'admet qu'un nombre fini des points entiers.

Remarque 1.0.1. Les résultats de Thue et Siegel ne sont pas effective, autrement dit qu'ils ne fournissent pas une méthode qui permet d'obtenir en un nombre fini d'opérations toutes les Solutions.

Vers la fin de la décennie soixante, A. Baker [7] a obtenu des bornes inférieurs explicites des formes linéaires en logarithme des nombres algébriques, qu'il a utilisé pour donner une preuve effective au théorème de Thue. Avec sa méthode, Baker est parvenu à résoudre de nombreuses équations diophantiennes de façon effective. Il a parachevé également la preuve de la conjecture de Gauss sur le nombre des classes dans le cas de corps quadratiques imaginaires dont le nombre des classes est 1.
Les résultats de Baker ont redynamisé l'analyse diophantienne. Il faut noter que les bornes qui surviennent dans la méthode de Baker sont énormes et il existe des méthodes pour les réduire en pratique.

E 1969, A. Schinzel a combiné le résultat de Siegel mentionné ci dessus et le théorème de Runge pour obtenir une amélioration de ce dernier.
R. Tijdeman [76] (1976) a démontré en utilisant une version de la méthode de Baker que l'équation de Catalan n'admet qu'un nombre fini des solutions.

En 1983, G. Faltings [26] a démontré, en utilisant des résultats de la géométrique algébrique, la conjecture de Mordell (déjà mentionné plus haut). C'est l'un des résultats mathématiques le plus remarquable et le plus profond de la deuxième moitié du $20^{ème}$ siècle. Comme conséquence du résultat de Faltings, l'équation de Fermat n'admet qu'un nombre fini des solutions.

Après plus de trois siècles et demi, la conjecture de Fermat, qu'on appelait dernier théorème de Fermat est enfin devenu un théorème. En effet, en 1995, A. Wiles et R. Taylor [81] ont corrigé quelques imperfections apparaissant dans une preuve de Wiles (1993) de la conjecture de Shimura-Taniyama-Weil pour les courbes elliptiques semi-stables. Il était montré quelques années plutôt que la justesse de cette conjecture impliquerait le dernier théorème de Fermat suite aux travaux des mathématiciens G. Frey, J. P. Serre et K. Ribet.
La méthode de Wiles permet aussi de résoudre d'autres types d'équations diophantiennes.

En 2003, P. Mihăilescu [53] est parvenu, en utilisant principalement la méthode de Runge et la théorie des corps cyclotomiques, à démontrer la conjecture de Catalan.

Des nombreux auteurs ont considérés des questions similaires à celles présentées dans cette thèse. On peut citer, par exemple, István Gaál et Michael Pohst (2008) ; Y. Hu et M. Le (2013) ; K. Keskin, Z. ¸Siar, et O. Karaatli (2013) ; O. Beckwith (2017).

Organisation de la thèse et contributions

Cette thèse contient quatre chapitres et dans chaque chapitre, à part le chapitre I, nous présentons un nouveau résultat.
Le chapitre I est une introduction générale. Il contient un bref historique de l'analyse diophantienne, des problèmes traités dans la thèse et l'organisation de ce présent mémoire.
Le chapitre II comprend trois sections. La première section concerne le résultant de deux polynômes. La deuxième section présente la méthode de Runge et son amélioration par Schinzel. Enfin, dans la troisième section nous utilisons les résultats de deux sections précédentes pour montrer que l'équation diophantienne

$$Res_x(P(x), x^2 + sx + t) = a$$

admet un nombre fini de solutions entières, où

$$P(x) = a_m(x - \alpha_1)\cdots(x - \alpha_m),$$

$a_m \in \mathbb{Z}$, α_i sont les racines de P dont au moins trois sont distinctes ; Res_x est le résultant en x de deux polynômes et où s, t et a sont des entiers rationnels.
Le chapitre III est subdivisé aussi en trois sections. Nous faisons d'abord quelques rappels sur les fractions continues dans la première section. La deuxième section est consacrée à la théorie des équations de Pell-Fermat. Dans la troisième section nous étudions l'équation diophantienne

$$x^2 - kxy + ky^2 + ly = 0,$$

où k et l sont des entiers avec k pair. Nous donnons une caractérisation des solutions entières positives de cette équation en fonction de k et l. En effet, nous montrons le

théorème suivant.

Théorème 1.0.2. *Soient l et k des entiers, avec k pair. Si $l^2 < k$, alors l'équation diophantienne $x^2 - kxy + ky^2 + ly = 0$ admet une infinité des solutions entières positives x et y si et seulement si $(l,k) = (2,6)$. De plus, les solutions sont données par les suites (où $x_n = x$ et $y_n = y$)*

$$\begin{cases} x_n &= \dfrac{v_n - u_n}{2} - 1 \\ y_n &= -\dfrac{1}{6}(u_n - 2) \end{cases}$$

où n est impair et u_n, v_n sont donnés par les suites suivante

$$\begin{cases} u_n &= -2((2)^n + \displaystyle\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (2)^{n-2i} (3)^i) \\ v_n &= \pm 2(\displaystyle\sum_{i=1}^{\frac{n+1}{2}} \binom{n}{2i-1} (2)^{n-2i+1} (3)^{i-1}) \end{cases}$$

Nous considérons aussi la même équation quand $l = 3^n$ et $k \equiv 2$ (modulo 3) ; $l = 2^r 3^s$ et $k = 2k' + 1$ avec $k' \equiv 2$ (modulo 3) où n, r et s sont des entiers positifs. Nos résultats généralisent en particulier ceux de Karaatli et Şiar [41]. Les résultats de ce chapitre sont contenus dans Alkabouss et al [2]

Le chapitre IV est également divisé en trois sections. La première section concerne la théorie des formes quadratiques binaires. Dans la deuxième section nous donnons quelques rappels de la théorie algébrique des nombres en nous focalisant surtout sur la décomposition des nombres premiers dans les corps de nombres et le nombre des classes. Dans la dernière sections nous présentons une borne inférieure sur les $h+1$ premiers nombres premiers qui se décomposent dans un corps quadratique imaginaire où h désigne le nombre de classes de ce corps. En effet, nous démontrons le théorème suivant.

Théorème 1.0.3. *Soit D un entier tel que $D < 0$ et $D \equiv 0,1 (\mathrm{mod}\ 4)$. Soit $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ et $h_{\mathbb{K}}$ le nombre des classes de $\mathbb{K}$. Alors, les $h_{\mathbb{K}} + 1$ plus petits nombres premiers impairs qui se décomposent dans $\mathbb{K}$ vérifient l'inégalité suivante :*

$$p_{h_{\mathbb{K}}+1} \geq \frac{1}{4}\sqrt{3|D|}$$

.

Publications et Soumissions :

1) On the equation $Res_x(P(x), x^2 + sx + t) = a$, International Journal of Number Theory, Vol. 14, No. 4 (2018) 1073–1079. ©World Scientific Publishing Company. DOI : 10.1142/S1793042118500653. (Join work with T. Garici and J. Larone).
2) A note on the Diophantine equation $x^2 - kxy + ky^2 + ly = 0$. (Join work with B. Benseba and B. Nacera)(Soumis).
3) On the small primes that split in certain imaginary quadratic fields. (Join work with B. Benseba and B. Nacera)(Soumis).

Chapitre 2

La méthode de Runge et équation diophantienne de forme résultant

Dans ce chapitre, nous montrons que l'équation diophantienne du type résultant admet un nombre fini de solutions entières, autrement dit que l'équation $\mathrm{Res}(P,Q) = a$, où P et Q sont des polynômes et a un entier, n'a qu'un nombre fini de solutions entières. Notre démonstration utilise un résultat de Schinzel [66] améliorant le théorème de Runge [64]. Ce résultat est contenu dans Alkabouss et al [4]. Le chapitre est organisé de la manière suivante : la première section est consacrée au résultant de deux polynômes. Puis dans la seconde section nous présentons le théorème de Runge et son amélioration par Schinzel et enfin, dans la dernière section nous étudions l'équation diophantienne du type résultant.

2.1 Le résultant de deux polynômes

Le résultant est un outils essentiel dans de nombreux domaines de mathématiques qui traitent des polynômes. En effet, il est utilisé dans l'analyse diophantienne, la géométrie algébrique, le calcul formel, la théorie algébrique des nombres, entre autres.
Soient A un anneau commutatif unitaire et $\mathbb{K}$ son corps des fractions. Soient

$$P(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_0$$

et

$$Q(x) = b_n x^n + b_{n-1} x^{n-1} + ... + b_0$$

deux polynômes à coefficients dans A de degré m et n respectivement. La matrice de Sylvester de P et Q est la matrice carré de taille $(m+n) \times (m+n)$ définie comme suit :

$$Syl(P,Q) = \begin{pmatrix} a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & \cdots & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & \cdots & b_0 & 0 & \cdots & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_n & b_{n-1} & \cdots & \cdots & b_0 \end{pmatrix}$$

Définition 2.1.1. *Le résultant des deux polynômes P et Q est le déterminant de leur matrice de Sylvester, noté souvent par $Res_x(P,Q)$ s'il est nécessaire de préciser l'inconnue.*

Une autre définition, que l'on adoptera dans la suite de la thèse, est donnée en fonction des racines des polynômes P et Q. En effet, soient $\alpha_1, \alpha_2, \cdots, \alpha_{m-1}, \alpha_m$ et $\beta_1, \beta_2, \cdots, \beta_{n-1}, \beta_n$ les racines de P et Q, respectivement, dans une clôture algébrique de $\mathbb{K}$, alors :

Définition 2.1.2. *Le résultant de P et Q est donné par*

$$\text{Res}(P,Q) = a_m^n b_n^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j).$$

Pour la suite, nous donnons quelques propriétés du résultant sans preuves, ces dernières peuvent être trouvées par exemple dans Lang [47].

Proposition 2.1.1. *Soient $P(x)$ et $Q(x) \in A[x]$ deux polynômes de degrés m et n respectivement. Alors, il existe des polynômes $\phi(x)$ et $\psi(x) \in A[x]$ vérifiant $deg(\phi(x)) < n$ et $deg(\psi(x)) < m$ tels que*

$$\phi(x)P(x) + \psi(x)Q(x) = Res(P,Q)$$

Une conséquence importante de la proposition précédente est le critère de Sylvester qui dit que deux polynômes quelconques admettent un facteur non trivial en commun si et seulement si leur résultant est nul.

Proposition 2.1.2. *Soient $P(x)$ et $Q(x) \in A[x]$ deux polynômes de degrés m et n et dont les racines sont données par $\alpha_1, \alpha_2, \cdots, \alpha_{m-1}, \alpha_m$ et $\beta_1, \beta_2, \cdots, \beta_{n-1}, \beta_n$, respectivement dans une clôture algébrique de $\mathbb{K}$, alors nous avons les propriétés suivantes :*

1) $\mathrm{Res}(P,Q) = (-1)^{mn}\mathrm{Res}(Q,P)$.

2) $\mathrm{Res}(P,Q) = a_m^n \prod_{i=1}^m Q(\alpha_i) = (-1)^{mn} b_n^m \prod_{j=1}^n P(\beta_j)$.

3) $\mathrm{Res}(P,Q_1Q_2) = \mathrm{Res}(P,Q_1)\mathrm{Res}(P,Q_2)$.

2.2 La méthode de Runge

Dans cette section nous présentons le théorème de Runge (méthode) et le théorème de Schinzel qui améliore en quelque sorte (qualitativement) ce résultat.
On donne d'abord quelques définitions de certaines termes utilisés.

Définition 2.2.1. *Soit le polynôme $P(x) = a_n x^n + \cdots + a_0$ de $\deg(n)$. On appelle hauteur de P, le nombre donné par $h(P) = \max_{i=1,\cdots,n} |a_i|$.*

Soit K un corps commutatif. Il est connu que l'ensemble de séries formelles muni de la somme des séries et le produit de Cauchy des série forme un anneau $\mathbb{K}[[X]]$. Son corps de fractions est noté par $\mathbb{K}((X))$. On donne cette définition non rigoureuse des séries de Puiseux, tirée d'Arnaudies [6].

Définition 2.2.2. *Une série de Puiseux est une série formelle de la forme*

$$\sum_{i=-\infty}^{\infty} a_i x^{\frac{i}{N}}$$

où N est entier strictement positif et $a_i \in \mathbb{K}((XX))$. L'entier N est dépendant de la série de Puiseux considérée.

Remarque 2.2.1. Les séries de Puiseux sont, en fait, des séries formelles à exposants fractionnaires.

2.2.1 Théorème de Runge

C. Runge a prouvé dans [64], en 1887, le premier résultat général portant sur les solutions entières d'une équation diophantienne à deux inconnues.
Son résultat fournit une méthode pour résoudre des nombreuses équations diophantiennes, dont l'exemple le plus populaire qui l'utilise est la preuve par P. Mihăilescu en 2000 de la célèbre conjecture de Catalan.
La version générale du théorème de Runge s'énonce comme suit.

Théorème 2.2.1. *Soit*

$$F(x,y)=\sum_{i=0}^{m}\sum_{j=0}^{n}a_{ij}x^{i}y^{j}$$

un polynôme à coefficients entiers rationnels, irréductible dans $\mathbb{Q}[x,y]$*, avec* $deg_xF = m>0$ *et* $deg_yF = n>0$*. Supposons que l'équation diophantienne* $F(x,y)=0$ *admet une infinité des solutions entières* x,y*. Alors, ils existent des entiers* m,n *tels que :*

1) $a_{mj}=a_{in}=0\,\forall(i,j)>(0,0)$
2) $a_{ij}=0$ *pour toute paire* (i,j) *vérifiant* $ni+mj>mn$
3) *La somme* $\sum_{ni+mj=mn}a_{ij}x^{i}y^{j}$ *est à une constante multiplicative prés une puissance d'un polynôme irréductible dans* $\mathbb{Z}[x,y]$
4) *La fonction algébrique* $y=y(x)$ *définie par l'équation* $F(x,y)=0$ *admet un seul système de conjugués des développements de Puiseux à l'infini.*

Remarque 2.2.2. Dans [1], Ayad énonce le théorème de Runge comme étant le point 4) du théorème précédent, qui implique les trois autres points par ailleurs. Il en fournit une amélioration également.

Une conséquence du théorème de Runge est le corollaire suivant qui porte, d'ailleurs, le nom du théorème de Runge dans certains ouvrages, par exemple c'est le Théorème 21 à la page 276 dans Mordell [56].

Corollaire 2.2.2. *Avec les mêmes hypothèses que le théorème, si l'équation* $F(x,y)=0$ *admet une infinité des solutions entières alors la partie homogène dominante de* $F(x,y)$ *est à une constante multiplicative prés une puissance d'un polynôme irréductible.*

Si au moins un des points du théorème précédent n'est pas vérifié, alors l'équation admet un nombre fini des solutions entières. De plus, la méthode de Runge est effective,

dans le sens où des bornes supérieures sur la taille des solutions peuvent être obtenues. En effet, Hilliker et Strauss [37] ont obtenu de telles bornes en fonction de degré et la hauteur du polynôme $F(x,y)$. Walsh [77] a obtenu une amélioration de ce résultat.

2.2.2 Amélioration du théorème de Runge

En 1929, C. L. Siegel a démontré le résultat définitif qui permet de savoir si une équation algébrique donnée par $F(x,y) = 0$ admet une infinité de solutions entières. En effet, il démontra le théorème suivant :

Théorème 2.2.3 (Siegel)**.** *Si $F(x,y) = 0$ admet une infinité de solutions entières, alors ils existent des fonctions rationnels $u(t)$ et $v(t)$ dont au moins une n'est pas constante tels que*

$$F(u(t), v(t)) = 0$$

identiquement en t et soit

a)

$$u(t) = \frac{g(t)}{\alpha(t)^m}, \quad v(t) = \frac{h(t)}{\alpha(t)^m}$$

ou

b)

$$u(t) = \frac{G(t)}{\beta(t)^m}, \quad v(t) = \frac{H(t)}{\beta(t)^m}$$

où g, h, G, H, α et β sont des polynômes à coefficients entiers ; α est linéaire et β est quadratique irréductible et indéfini.

En 1969, A. Schinzel a obtenu une amélioration du théorème 4.1.6 en combinant le corollaire 2.2.2 et théorème de Siegel. Plus précisément, il a prouvé le théorème suivant :

Théorème 2.2.4. *Si $f(x,y)$ est un polynôme à coefficients entiers irréductible dans $\mathbb{Q}[x,y]$ et si l'équation $f(x,y) = 0$ admet une infinité des solutions entières alors la partie homogène dominante de $f(x,y)$ est à un facteur constant près une puissance linéaire ou une puissance d'une forme quadratique indéfinie irréductible.*

Remarque 2.2.3. Contrairement au théorème de Runge, le résultat de Schinzel n'est pas effectif car le théorème de Siegel qu'il utilise est non effective.

2.3 L'équation diophantienne de forme résultant

Dans cette section, nous démontrons en appliquant les résultats de sections précédentes que l'équation diophantienne de forme résultant admet un nombre fini des solutions entières.

Soit

$$P(x) = a_m(x-\alpha_1)\cdots(x-\alpha_m),$$

où $a_m \in \mathbb{Z}$ et α_i les racines de P. Soit

$$Q(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0 \in \mathbb{Z}[x],$$

alors d'après la définition du résultant donné plus haut, nous avons

$$\mathrm{Res}(P,Q) = a_m^n \prod_{i=1}^{m} (b_n\alpha_i^n + b_{n-1}\alpha_i^{n-1} + \cdots + b_0). \tag{2.3.1}$$

Nous considérons l'équation du type résultant donnée par

$$\mathrm{Res}(P,Q) = a, \tag{2.3.2}$$

où a est une entier rationnel donné non nul. Notons que l'équation du type résultant peut être considérée comme une équation diophantienne polynomiale en termes des coefficients de Q.

2.3.1 État de l'art

Plusieurs auteurs ont étudié l'équation diophantienne de forme résultant. Nous pouvons citer par exemple Wirsing [82], Fujiwara [27], Schmidt [68], Schlickewei [67], Pethő [61, 62], Győry [33], Evertse and K. Győry [25]-[24], Gaál [28] qui ont montré que le nombre des polynômes Q vérifiant l'équation (2.3.2) est fini sous la condition $m > n$.

En effet, Wirsing [82] (1971) a montré que si n est un entier positif tel que

$$2n\left(1+\frac{1}{3}+\cdots+\frac{1}{2n-1}\right)<m,$$

alors il n'y a qu'un nombre fini des polynômes $Q\in\mathbb{Z}[x]$ de degré n satisfaisant l'équation (2.3.2).

Une année plus tard, Fujiwara [27] a montré que si le polynôme P est irréductible sur $\mathbb{Q}$ et $2n<m$ alors l'équation (2.3.2) admet seulement un nombre fini de solutions $Q\in\mathbb{Z}[x]$ de degré n.

En 1973, Schmidt [68] a montré que l'irréductibilité de P peut être remplacée par la condition que P n'a aucun facteur non constant de degré inférieur ou égal à n dans $\mathbb{Z}[x]$.

Soient R un sous-anneau de $\mathbb{Q}$ qui est une extension d'anneau de type fini de $\mathbb{Z}$, a un élément non nul de R, et R^* le groupe des unités de R. Si m et n sont des entiers positifs tels que $2n<m$ et $P\in R[x]$ un polynôme de degré m sans racines multiple et qui n'admet pas un facteur non constant dans $R[x]$ de degré inferieur ou égal à n, alors a un facteur proportionnel de R^* prés, Schlickewei [67] a prouvé qu'il existe seulement un nombre fini des polynômes $Q\in R[x]$ de degré n vérifiant

$$\mathrm{Res}(P,Q)\in a\cdot R^*.$$

Győry [33] a montré que si $Q(x)$ est tel que son facteur dominant est égal à 1, alors la condition $m\geq 2n$ peut remplacer la condition $m>2n$. Voire le théorème 2 dans [33].

En 2002, Gaál [28], en utilisant la méthode de Baker (bornes inférieures de formes linéaires en logarithme des nombre algébriques), a développé un algorithme pour résoudre l'équation (2.3.2), quand $P\in\mathbb{Z}[x]$ est un polynôme irréductible de degré $m\geq 3$ et $Q=x^2+x_1x+x_2\in\mathbb{Z}[x]$. En fait, il a transformé l'équation (2.3.2)en une équation de

Thue non homogène

$$a_0^2 N_{F/\mathbb{Q}}(x_2 + x_1\alpha + \alpha^2) = a \quad \text{in } x_1, x_2 \in \mathbb{Z},$$

où α est une racine de P et $F = \mathbb{Q}(\alpha)$.
En 2008, Gaál et Posht [29] ont étendu le travail de Gaál à tout polynôme unitaire Q de degré $n \geq 2$.

Nous avons démontré dans [4], en utilisant le théorème de Schinzel 2.2.4 qui est une amélioration du théorème de Runge, que si P est un polynôme de degré m ayant au moins trois racines différentes alors l'équation diophantienne

$$\mathrm{Res}_x(P(x), x^2 + sx + t) = a$$

admet un nombre fini de solutions entières.
Notre résultat est non effective à cause de l'usage dans la preuve du théorème de Schinzel 2.2.4. En d'autre termes, nous ne pouvons pas obtenir des bornes supérieures sur la taille des solutions.

2.3.2 Résultats intermédiares

Soit

$$P(x) = a_m(x - \alpha_1)\cdots(x - \alpha_m) \in \mathbb{Z}[x],$$

où $a_m \in \mathbb{Z} \setminus \{0\}$ et α_i les racines de P. Nous considérons l'équation diophantienne de type résultant

$$R(s,t) = \mathrm{Res}_x(P(x), x^2 + sx + t) = a, \tag{2.3.3}$$

où a est un entier non nul donné.

Lemme 2.3.1. *Soient $A(s,t)$, $B(s,t) \in \mathbb{Z}[s,t]$ tel que*

$$P(x) = (x^2 + sx + t)q(s,t,x) + A(s,t)x + B(s,t),$$

alors

$$R(s,t) = B^2(s,t) + tA^2(s,t) - sA(s,t)B(s,t).$$

Démonstration. Considérons γ, $\beta = -s-\gamma$ les racines de x^2+sx+t dans une clôture algébrique de $\mathbb{Q}(s,t)$. Alors, nous avons

$$\begin{aligned} R(s,t) &= \mathrm{Res}_x\left(x^2+sx+t, P(x)\right) = P(\gamma)P(\beta) \\ &= (A\gamma+B)(A\beta+B) = tA^2+B^2-sAB. \end{aligned}$$

□

Ce lemme nous permet de déduire que $R(s,t) \in \mathbb{Z}[s,t]$. Donc il existe un unique polynôme $r_i(s) \in \mathbb{Z}[s]$ tel que $R(s,t) = \sum_{i=0}^{n} r_i(s)\,t^i$. De plus, de l'équation (2.3.1) nous avons

$$R(s,t) = a_m^2 \prod_{k=1}^{m} \left(\alpha_k^2 + s\alpha_k + t\right)$$

Alors $n = m$ et les deux polynômes $R(s,t)$ et $P(x)$ satisfont l'identité suivante

$$R(s,-x^2-sx) = P(x)P(-s-x) \tag{2.3.4}$$

Ainsi

$$\begin{aligned} P(x)P(-s-x) &= \sum_{i=0}^{m} (-1)^i r_i(s)\left(x^2+sx+t-t\right)^i \\ &= \sum_{k=0}^{m}\left(\sum_{i=k}^{m}\binom{i}{k}(-1)^k t^{i-k} r_i(s)\right)\left(x^2+sx+t\right)^k \end{aligned}$$

A partir de cela nous déduisons l'existence des polynômes $u_k(s,t) \in \mathbb{Z}[s,t]$ tels que

$$P(x)P(-s-x) = u_0(s,t) + u_1(s,t)(x^2+sx+t) + \cdots + u_m(s,t)(x^2+sx+t)^m,$$

avec $u_0(s,t) = R(s,t)$ and $u_m(s,t) = (-1)^m a_m^2$. Plus généralement, nous avons la proposition suivante.

Proposition 2.3.2. *Soient $s,\ t,\ x$ 3 variables algébriquement indépendantes sur $\mathbb{Q}$. Si $Q(x)$ est un polynôme à coefficients dans $\mathbb{Z}[s,t]$ vérifiant $Q(-s-x) = Q(x)$, alors :*

1. *Il existe un unique* $v_k(s,t) \in \mathbb{Z}[s,t]$ *tel que*

$$Q(x) = v_0(s,t) + v_1(s,t)(x^2+sx+t) + \cdots + v_h(s,t)(x^2+sx+t)^h.$$

2. $\mathrm{Res}_x\left(Q(x), x^2+sx+t\right) = (v_0(s,t))^2$

Démonstration. L'unicité est évidente car, il s'agit d'une représentation (x^2+sx+t)-adique de $Q(x)$. C'est une représentation particulière parce que les coefficients v_0, $v_1, \ldots, v_h$ dépendent seulement de s et t mais pas de x. Soient $q(s,t,x)$, $w(s,t)$ et $v_0(s,t)$ l'unique polynômes à coefficient dans $\mathbb{Z}$ tels que

$$Q(x) = q(s,t,x)(x^2+sx+t) + w(s,t)x + v_0(s,t).$$

Alors l'égalité $Q(-s-x) = Q(x)$ et l'unicité des polynômes q, w, v_0 impliquent que $w = 0$. Ainsi $Q(x) = v_0(s,-x^2-sx)$. Posons $v_0(s,t) = \sum_{i=0}^{h} r_i(s)\,t^i$, alors

$$Q(x) = \sum_{k=0}^{h}\left(\sum_{i=k}^{h}\binom{i}{k}(-1)^k t^{i-k} r_i(s)\right)(x^2+sx+t)^k$$

Nous pouvons en déduire qu'il existe un polynôme $v_k(s,t) \in \mathbb{Z}[s,t]$ tel que

$$Q(x) = v_0(s,t) + v_1(s,t)(x^2+sx+t) + \cdots + v_h(s,t)(x^2+sx+t)^h,$$

où pour chaque k,

$$v_k(s,t) = \sum_{i=k}^{h}\binom{i}{k}(-1)^k t^{i-k} r_i(s).$$

Soient γ, β les zéros de x^2+sx+t dans une clôture algébrique $\mathbb{Q}(s,t)$, alors $Q(\gamma) = Q(\beta) = v_0(s,t)$ ainsi

$$\mathrm{Res}_x(Q(x), x^2+sx+t) = (v_0(s,t))^2.$$

□

De la proposition précédente, nous pouvons en déduire le résultat suivant.

Proposition 2.3.3. *L'équation* (2.3.3) *admet une solution* $(s^*, t^*) \in \mathbb{Z}^2$ *si et seulement si*

$$P(x)P(-s^*-x)-a \equiv 0 \pmod{x^2+s^*x+t^*}.$$

Alors nous étudierons les valeurs de $s^* \in \mathbb{Z}$ pour lesquelles $P(x)P(-s^*-x)-a$ est réductible et possède un facteur quadratique.
Pour le polynôme $R(s,t)-a$, nous remarquons par la Proposition 2.3.2, que l'on peut écrire $P(X)+P(-s-X)$ sous la forme

$$P(x)+P(-s-x) = v_0(s,t)+v_1(s,t)(x^2+sx+t)+\cdots+v_h(s,t)(x^2+sx+t)^h.$$

Proposition 2.3.4. *Soit*

$$r(s,t) = \mathrm{Res}_x\left(P(x)+P(-s-x)-v_0(s,t), P(x)P(-s-x)-a\right),$$

alors

$$r(s,t) \equiv 0 \pmod{(R(s,t)-a)^2}.$$

Démonstration. Considérons

$$V(x,s,t) = v_1(s,t)+\cdots+v_h(s,t)(x^2+sx+t)^{h-1},$$

et

$$R_1(s,t) = \mathrm{Res}_x((x^2+sx+t), P(x)P(-s-x)-a).$$

Donc nous avons

$$P(x)+P(-s-x)-v_0(s,t) = (x^2+sx+t)V(x,s,t)$$

et

$$r(s,t) = \mathrm{Res}_x\left(V(x,s,t), P(x)P(-s-x)-a\right) R_1(s,t). \tag{2.3.5}$$

Soient γ, $\beta = -s-\gamma$ les racines de x^2+sx+t dans la clôture algébrique de $\mathbb{Q}(s,t)$. Alors nous avons

$$R(s,t) = \mathrm{Res}_x\left(x^2+sx+t, P(x)\right) = P(\gamma)P(-s-\gamma)$$

et

$$R_1(s,t) = \big(P(\gamma)P(-s-\gamma)-a\big)^2 = (R(s,t)-a)^2$$

Ainsi

$$r(s,t) = \mathrm{Res}_x(V(x,s,t), P(x)P(-s-x)-a)\,(R(s,t)-a)^2$$

Nous concluons que $r(s,t) \equiv 0 \pmod{(R(s,t)-a)^2}$.

□

2.3.3 Irréductibilité du polynôme $R(s,t)-a$, pour a fixé dans $\mathbb{Z}\setminus\{0\}$

Dans cette section, nous étudions l'irréductibilité du polynôme $R(s,t)-a$, où a est entier non nul fixé.

Théorème 2.3.5. *Soient $a \in \mathbb{Z}\setminus\{0\}$, $P(x) \in \mathbb{Z}[x]$ un polynôme séparable de degré m, et $Q(s,x) \in \mathbb{Z}[s,x]$ un polynôme de la forme*

$$Q(s,x) = Q_n s^n + Q_{n-1}(x)s^{n-1} + \cdots + Q_0(x),$$

avec $n \geq 1$ et $Q_n \in \mathbb{Z}\setminus\{0\}$. Alors le polynôme $P(x)Q(s,x)-a$ est absolument irréductible.

Démonstration. Soient

$$A(s,x) = A_k(x)s^k + A_{k-1}(x)s^{k-1} + \cdots + A_0(x)$$

et

$$B(s,x) = B_\ell(x)s^\ell + B_{\ell-1}(x)s^{\ell-1} + \cdots + B_0(x)$$

deux polynômes dans une clôture algébrique de $\mathbb{Q}[x,s]$ tels que $k \geq \ell$, $k+\ell = n$ et

$$P(x)Q(s,x) - a = A(s,x)B(s,x) \tag{2.3.6}$$

Supposons maintenant que $\ell \geq 1$ et $k+\ell = n$. Par identification des coefficients de s^j,

pour $j = 0, 1, \ldots, n$, nous obtenons

$$\begin{aligned} P(x)Q_n &= A_k(x)B_\ell(x), \\ P(x)Q_{n-1}(x) &= A_k(x)B_{\ell-1}(x) + A_{k-1}(x)B_\ell(x), \\ &\cdots \\ P(x)Q_j(x) &= \sum_{\substack{u+v=j \\ u\le k,\, v\le \ell}} A_u(x)B_v(x), \quad \text{avec} \quad j = n-2, \ldots, 1, \\ &\cdots \\ P(x)Q_0(x) - a &= A_0(x)B_0(x). \end{aligned} \tag{2.3.7}$$

Comme $P(x)$ est séparable, alors $(A_k(x), B_\ell(x)) = 1$. La deuxième équation dans (2.3.7) montre que $A_k(x)|A_{k-1}(x)$ et $B_\ell(x)|B_{\ell-1}(x)$. Les équations suivantes donnent $A_k(x)|A_j(x)$ et $B_\ell(x)|B_h(x)$, pour $j = 0, \ldots, k-1$ et$h = 0, \ldots, \ell-1$. Cela contredit la dernière équation dans (2.3.7). Ainsi, de cela, nous pouvons conclure que $\ell = 0$, donc $B(s,x) = B(x)$ et $k = n \ge 1$. En identifiant les coefficients des s^n et s^0 dans (2.3.6), nous obtenons

$$a = B(x)\left(\frac{1}{Q_n}Q_0(x)A_n(x) - A_0(x)\right)$$

Cela implique que $B(x)$ est un polynôme constant. □

Nous déduisons les résultats suivants.

Corollaire 2.3.6. *Soient $a \in \mathbb{Z} \setminus \{0\}$ et $P(x) \in \mathbb{Z}[x]$ un polynôme séparable, alors le polynôme $P(x)P(-s-x) - a$ est absolument irréductible.*

Démonstration. C'est un cas particulier du théorème 2.3.5 avec $Q(s,x) = P(-s-x)$. □

Corollaire 2.3.7. *Supposons que $a \in \mathbb{Z} \setminus \{0\}$ et $P(x) \in \mathbb{Z}[x]$ un polynôme séparable. Soit*

$$R(s,t) = \mathrm{Res}_x(P(x), x^2 + sx + t).$$

Alors le polynôme $R(s,t) - a$ est absolument irréductible.

Démonstration. Par la relation(2.3.4),

$$R(s, -x^2 - sx) - a = P(x)P(-s-x) - a$$

qui est absolument irréductible d'après le Corollaire 2.3.6, ainsi nous avons que $R(s,t)-a$ est absolument irréductible.

□

2.3.4 Application de la méthode de Runge

Dans cette section, nous utiliserons la méthode de Runge pour montrer que l'équation (2.3.2) admet un nombre fini des solutions entières, plus précisément nous utiliserons le Théorème 2.2.4 de Schinzel.
Pour pouvoir appliquer le Théorème 2.2.4, il nous faut déterminer la partie homogène dominante de

$$R(s,t) = \mathrm{Res}_x(P(x), x^2+sx+t).$$

Le lemme suivant nous permet de la déterminée.

Lemme 2.3.8. *Soient $P(x) \in \mathbb{Z}[x]$,*

$$R(s,t) = \mathrm{Res}_x(P(x), x^2+sx+t)$$

et $R^+(s,t)$ sa partie homogène dominante. Alors

$$R^+(s,t) = a_m(-s)^m P(-t/s),$$

où $m = \deg P$ et a_m est le coefficient dominant de $P(x)$.

Démonstration. Soient $\alpha_1,\ldots,\alpha_m$ les racines de $P(x)$. Alors nous avons

$$R(s,t) = \mathrm{Res}_x\left(P(x), x^2+sx+t\right) = a_m^2 \prod_{i=1}^{m}(\alpha_i^2+s\alpha_i+t).$$

Donc

$$\begin{aligned} R^+(s,t) &= a_m^2 \textstyle\prod_{i=1}^m (s\alpha_i+t) = a_m^2 \prod_{i=1}^m (-s)\left(-\alpha_i - \frac{t}{s}\right) \\ &= (-s)^m a_m \cdot a_m \textstyle\prod_{i=1}^m \left(-\alpha_i - \frac{t}{s}\right) = a_m(-s)^m P(-t/s). \end{aligned}$$

□

Théorème 2.3.9. *Supposons que $b \in \mathbb{Z}\setminus\{0\}$ et $f(x) \in \mathbb{Z}[x]$. Si $\deg f - \deg\left(\gcd\left(f, f'\right)\right) \geq 3$*

alors l'équation

$$\mathrm{Res}_x\left(f(x), x^2+sx+t\right) = b \tag{2.3.8}$$

admet un nombre fini des solutions entières.

Démonstration. Soit $D = \gcd(f, f')$, et posons $P(x) = \frac{f(x)}{D(x)}$. Alors $P(x)$ est séparable, $\deg P \geq 3$ et

$$\mathrm{Res}_x(f(x), x^2+sx+t) = R(s,t)\,\mathrm{Res}_x\left(D(x), x^2+sx+t\right).$$

L'équation (2.3.8) implique qu'il existe un diviseur a de b tel que :

$$R(s,t) = a \tag{2.3.9}$$

Posons $F(s,t) = R(s,t) - a$, alors d'après le corollaire 2.3.7, $F(s,t)$ est irréductible et par le Lemme 2.3.8, nous avons

$$F^+(s,t) = R^+(s,t) = a_m(-s)^m P(-t/s).$$

où $m = \deg P$ et a_m est le coefficient dominant de $P(x)$. Les conditions du Théorème de Schinzel 2.2.4 ne sont pas remplies. Donc l'équation (2.3.9) admet un nombre fini des solutions entières. Ainsi les diviseurs de b sont en nombre fini, et que l'équation (2.3.8) admet un nombre fini des solutions entières. □

Chapitre 3

Équations diophantiennes de la forme $x^2 - kxy + ky^2 + ly = 0$

Dans ce présent chapitre nous étudions l'équation diophantienne suivante

$$x^2 - kxy + ky^2 + ly = 0$$

pour des valeurs entières de k et l. Dans un premier temps, nous donnons une caractérisation des solutions entières positives de cette équation en fonction de k et l avec k paire. Puis nous la considérons quand $l = 3^n$ et $k \equiv 2$ (modulo 3) ; $l = 2^r 3^s$ et $k = 2k' + 1$ avec $k' \equiv 2$ (modulo 3) où n, r et s sont des entiers positifs. L'étude de cette équation étant intimement liée à la théorie des équations de Pell-Fermat, nous donnons dans la première section des résultats sur les fractions continues et dans la deuxième section nous présentons quelques résultats nécessaires dans la suite du chapitre sur les équations de Pell-Fermat. Enfin, dans la dernière section nous présentons notre étude sur l'équation en question.

3.1 Fractions continues

Cette section est consacrée à l'étude de l'algorithme de fractions continues. La motivation principale de sa présentation ici est son utilisation dans la résolution de l'équation de Pell-Fermat. Nous referons à Bugeaud [16] Cassels [17] et Hardy et Wright [34] pour

les preuves des différents propriétés et résultats présentés ci-dessous.

3.1.1 Fractions continues : définitions et algorithme

Les fractions continues ou fractions continuées ont le don d'ubiquité en mathématiques. En effet, elles sont présentes dans des nombreux domaines tels que la théorie des nombres, l'analyse numérique, l'analyse complexe, la théorie des ensembles, la physique, la musique,...

Définition 3.1.1. *Une fraction continue finie décrit une expression de la forme :*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

où $a_0 \in \mathbb{R}$ et pour $i > 0$ $a_i \in \mathbb{R}_+$.

Remarque 3.1.1.

a) Nous utiliserons dans la suite la représentation moins embarrassante suivante d'une fraction continue à la place de la précédente $[a_0, a_1, a_2, \cdots, a_n]$

b) Si $a_0 \in \mathbb{Z}$ et pour $i > 0$ $a_i \in \mathbb{N}$ alors la fraction finie est dite simple.

La proposition suivante donne, en utilisant l'algorithme d'Euclide pour le calcul du $pgcd$ (plus grand commun diviseur) de deux entiers, la fraction continue d'un nombre rationnel.

Proposition 3.1.1. *Le nombre x peut être représenté par une fraction continue finie simple si et seulement si il est rationnel.*

Un autre résultat qui décrit exactement le développement en fraction continue d'un nombre rationnel est donné dans la proposition suivante.

Proposition 3.1.2. *Un nombre rationnel peut être représenté comme fraction continue en exactement deux manières, une de la forme* $[a_0, a_1, a_2, \cdots, a_n]$ *avec* $a_n \geq 2$ *et l'autre est donnée par* $[a_0, a_1, a_2, \cdots, a_{n-1} - 1, 1]$.

Nous avons la définition plus générale suivante d'une fraction continue.

Définition 3.1.2. *Une fraction continue infinie est définie par la limite suivante si elle existe.*

$$[a_0, a_1, a_2, \cdots,] = \lim_{n\to\infty} [a_0, a_1, a_2, \cdots, a_n]$$

où $a_0 \in \mathbb{R}$ *et pour* $i > 0$ $a_i \in \mathbb{R}_+$.

Remarque 3.1.2. Nous avons l'équivalent de la proposition 3.1.1 dans le cas infini, en effet, un nombre réel α peut être représenté par une fraction continue infinie simple si et seulement si il est irrationnel.

L'algorithme du calcul de la fraction continue d'un irrationnel α :
Soient $a_0 = [\alpha]$ la partie entière de α et $\alpha_1 = \dfrac{1}{\{\alpha\}}$ où $\{\alpha\}$ est la partie fractionnaire de α , donc $\alpha_1 > 1$. Donc

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

α_1 n'étant pas entier, il peut s'écrire à son tour sous la forme $\alpha_1 = a_1 + \frac{1}{\alpha_2}$ avec $\alpha_2 > 1$. Ainsi pour tout $n > 0$, on définit $a_n = [\alpha_n]$ et $\alpha_{n+1} = \dfrac{1}{\{\alpha_n\}}$ et $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$. Le processus ne s'arrête jamais car nous avons supposé que α est irrationnel. Ainsi, à tout nombre irrationnel est associé une fraction continue infinie simple $[a_0, a_1, a_2, \cdots,]$.

Définition 3.1.3. *On appelle réduite d'ordre* r *de la fraction continue* $[a_0, a_1, a_2, \cdots, a_n]$ *pour* $0 < r \leq n$ *la fraction continue tronquée à* $r + 1$ *coefficients, autrement dit*

$$\frac{h_r}{k_r} = [a_0, a_1, a_2, \cdots, a_r] = a_0 + \frac{1}{[a_0, a_1, a_2, \cdots, a_r]}.$$

Les coefficients a_n *sont appelés quotients partiels et les termes* α_n *les quotients complets.*

La proposition suivante permet de calculer la réduite d'une fraction continue par récurrence.

Proposition 3.1.3. *Posons $h_{-1} = 1$, $k_{-1} = 0$, $h_0 = a_0$, $k_0 = 1$ et définissons les suites $(h_n)_{n\geq 1}$ et $(k_n)_{\geq 1}$ par*

$$\begin{cases} h_n &= a_n h_{n-1} + h_{n-2} \\ k_n &= a_n k_{n-1} + k_{n-2} \end{cases}$$

Alors la réduite d'indice n est donnée par $\dfrac{h_n}{k_n} = [a_0, a_1, a_2, \cdots, a_n]$.

La proposition suivante nous garantit que les réduites d'une fraction continue sont écrites sous forme irréductible.

Proposition 3.1.4.

i) Soient $(h_n)_{n\geq 1}$ et $(k_n)_{n\geq 1}$ les suites définies dans la proposition précédente, alors nous avons

$$h_n k_{n-1} - h_{n-1} k_n = (-1)^{n-1}$$

ii) Elles vérifient également

$$h_n k_{n-2} - h_{n-2} k_n = (-1)^n a_n$$

Remarque 3.1.3. En notant par r_n la réduite d'indice n, autrement dit $r_n = \dfrac{h_n}{k_n}$, d'après la proposition précédent, nous avons :

i) $r_n - r_{n-1} = \frac{(-1)^n}{k_n k_{n-1}}$ et

i) $r_n - r_{n-2} = \frac{(-1)^n a_n}{k_n k_{n-2}}$

iii) Il est facile de voir que $1 = k_0 \leq k_1$ et $\forall\, n > 1, k_n < k_{n+1}$ et donc $\lim_{n\longrightarrow\infty} |r_n - r_{n-1}| = 0$

iv) Nous avons également $r_1 > r_3 > r_5 > \cdots > r_6 > r_4 > r_2$. En d'autres toute réduite d'indice impair est supérieure à toute réduite d'indice pair, les réduites d'indice pair forment une suite strictement croissante et que les réduites d'indice impair forment une suite strictement décroissante.

Proposition 3.1.5.

i) Soit $[a_0, a_1, a_2, \cdots,]$ le développement en fraction continue d'un irrationnel α et $r_n =$

$[a_0, a_1, a_2, \cdots, a_n]$ *sa réduite d'indice n alors*

$$|\alpha - r_n| \leq \frac{1}{k_n k_{n-1}} < \frac{1}{k_n^2}$$

ii)

$$\alpha = [a_0, a_1, a_2, \cdots, \alpha_{n+1}] = \frac{h_n \alpha_{n+1} + h_{n-1}}{k_n \alpha_{n+1} + k_{n-1}}$$

avec $\alpha_{n+1} = a_{n+1} + \dfrac{1}{\alpha_{n+2}}$ *comme définit plus haut.*

Proposition 3.1.6. *Soient* α *un nombre réel et* $\dfrac{u}{v}$ *un rationnel non nul. Si*

$$\left|\alpha - \frac{u}{v}\right| < \frac{1}{2v^2}$$

alors $\dfrac{u}{v}$ *est une réduite de la fraction continue de* α.

3.1.2 Fractions continues d'un irrationnel quadratique

Définition 3.1.4. *Une fraction continue infinie est périodique à partir du rang k s'il existe un entier positif l fixé tel que* $a_k = a_{k+l}$, *et on la note par*

$$[a_0, a_1, a_2, \cdots, a_{k-1}, a_k, a_{k+1}, a_{k+2}, \cdots, a_{k+l-1}\overline{a_k, a_{k+1}, a_{k+2}, \cdots, a_{k+l-1}}]$$

Le nombre l des quotients partiels répétés est appelé période de la fraction continue.

Le théorème suivant est d'une importance capitale dans la résolution de l'équation de Pell-Fermat. Le sens direct a été démontré par Euler et la réciproque par Lagrange.

Théorème 3.1.7. *Si le développement en fraction continue de* α *est périodique alors* α *est un irrationnel quadratique, en d'autre termes* α *est racine d'un polynôme quadratique à coefficients entiers. Réciproquement, si* α *est un irrationnel quadratique alors son développement en fraction continue est périodique.*

Il y arrive que certains irrationnels possèdent un développement en fraction continue purement périodique, c'est à dire périodique de le premier terme. Le théorème suivant, due à Galois, permet de savoir quand cela est possible.

Théorème 3.1.8. *Le développement en fraction continue de l'irrationnel quadratique α est purement périodique si et seulement si α est réduit, autrement dit $\alpha > 1$ et son conjugué α' vérifie $-1 < \alpha' < 0$.*

Proposition 3.1.9. *Si D est une entier positif sans facteur carré, alors le développement en fraction continue de $\sqrt{D}$ est donné par*

$$\sqrt{D} = [a_o, \overline{a_1, a_2, a_3, \cdots, a_3, a_2, a_1, 2a_0}]$$

3.2 Équation de Pell-Fermat

Dans cette section, nous présentons quelques résultats, nécessaires dans la suite, concernant les équations dites de Pell-Fermat, ceux sont les équations diophantiennes de la forme

$$X^2 - DY^2 = N \tag{3.2.1}$$

avec N un entier fixé et $D \geqslant 2$ n'est pas un carré parfait. Dans le cas $N = 1$, l'équation est dite de *Pell-Fermat*, on trouve souvent seulement le nom Pell dans la littérature. L'équation est dite de *Pell-Fermat négatif* dans le cas $N = -1$ et *Pell-Fermat généralisée* dans le cas N quelconque.

Ces équations ont une longue et riche histoire. En effet, des mathématiciens grecs de l'antiquité l'ont étudié pour approximer les nombres $\sqrt{2}$. Une autre preuve de son ancienneté, plus célèbre, est le problème de bœufs du soleil découvert par le littéraire et libraire allemand Lessing en 1773, attribué à Archimède. Le problème comprend d'une part, un système de sept équations linéaires à huit inconnues et d'autre part deux contraintes arithmétiques (une somme de deux inconnues doit être un carré et une autre de deux autres inconnues doit être un nombre triangulaire). En simplifiant, et en regroupant, on se ramène à une équation de Pell-Fermat.

Des avancées significatives, pour des valeurs particulières de D et N, ont été apportées par des mathématiciens indiens. Par exemple Brahmagupta, au septième siècle, a traité le cas $D = 61$, il a introduit la méthode *Bhāvanā* qui lui permet d'obtenir plusieurs solutions à partir de deux autres données. Il a été repris au douzième siècle par Bhāskara, qui a introduit une méthode cyclique, qui s'apparente à l'algorithme des

fractions continues, connue sous le nom *cakravāla*. Leurs travaux n'étaient connus en Europe qu'à partir de 1817.
Fermat l'a étudié au dix-septième siècle et conjectura que l'équation dans le cas $N = 1$ admet toujours une solution non triviale, autrement dit une solution (x, y) différente de $(\pm 1, 0)$. Il lança, pour des valeurs particulières de D, un défi au mathématicien anglais de son époque. Brouncker et Wallis avaient relevé avec brio le défi et ont introduit le lien avec les fractions continues. Euler a repris les travaux de Brouncker et Wallis et a , en plus, considéré les équations quadratiques plus générales. C'est d'ailleurs Euler qui l'a faussement nommé en l'honneur du mathématicien J. Pell sans aucune justification. Lagrange a finalement résolu le problème, en démontrant le théorème (3.1.7) du paragraphe précédent.
L'équation de Pell-Fermat est aussi intimement liée au groupe des unités d'un corps quadratique réel. En effet, elle permet de trouver l'unité fondamentale de ce corps. Nous y reviendrons avec plus détails sur ce groupe dans le chapitre suivant.

3.2.1 Équation de Pell-Fermat

Nous considérons maintenant l'équation

$$X^2 - DY^2 = 1. \tag{3.2.2}$$

Définition 3.2.1. *La plus petite solution positive $x + y\sqrt{D}$ autre que la solution triviale est appelée solution fondamentale de l'équation.*

Si D est un entier positif qui n'est pas un carré parfait, nous avons le théorème suivant.

Théorème 3.2.1. *Soit D un entier qui n'est pas un carré parfait, l'équation* (3.2.2) *admet une infinité des solutions entières $x + y\sqrt{D}$. Toutes les solutions avec x et y positives sont obtenu à partir de la formule*

$$x_n + y_n\sqrt{D} = (x_1 + y_1\sqrt{D})^n$$

où $x_1 + y_1\sqrt{D}$ est la solution fondamentale de l'équation ((3.2.2)*) et n parcourt l'ensemble des entiers naturels.*

D'après le théorème précédent, il suffit de connaitre la solution fondamentale de l'équation de Pell-Fermat pour les connaitre toutes. Ainsi, il nous faut un moyen pour la trouvée. La méthode élémentaire qui consiste à tester des valeurs particulières de X et Y n'est pas pratique, car pour certaines valeurs de D, même petite, la solution fondamentale est très grande. Heureusement, l'algorithme de fraction continue permet de trouver la solution fondamentale de l'équation.

En effet, soit $X + Y\sqrt{D}$ une solution de l'équation de Pell-Fermat

$$X^2 - DY^2 = \pm 1.$$

Alors

$$\left|X - Y\sqrt{D}\right| \left|X + Y\sqrt{D}\right| = 1.$$

Donc

$$\left|X - Y\sqrt{D}\right| = \frac{1}{X + Y\sqrt{D}}$$

et comme $X > Y\sqrt{D}$ Alors $\left|X - Y\sqrt{D}\right| < \dfrac{1}{2Y\sqrt{D}}$. D'où

$$\left|\sqrt{D} - \frac{X}{Y}\right| < \frac{1}{2Y^2}.$$

D'après le théorème (3.1.6) $\dfrac{X}{Y}$ est une réduite du développement en fraction continue de $\sqrt{D}$. Nous savons également par le théorème (3.1.9) que le développement en fraction continue de $\sqrt{D}$ est périodique à partir d'un certain rang et est donné par

$$\sqrt{D} = [a_o, \overline{a_1, a_2, a_3, \cdots, a_3, a_2, a_1, 2a_0}].$$

Le théorème suivant donne l'ensemble des solutions de l'équation (3.2.2) en termes des réduites de la fraction continue de $\sqrt{D}$

Théorème 3.2.2. *Soient l la période de la fraction continue de $\sqrt{D}$, n un entier positif et $\frac{h_n}{k_n}$ les réduites de la fraction continue de $\sqrt{D}$. Si l est pair alors toutes les solutions*

positives de l'équation (3.2.2)*, sont données par*

$$x = h_{nl-1}, \quad et \quad y = k_{nl-1}$$

alors qu'il n'y a pas des solutions à l'équation

$$X^2 - DY^2 = -1. \tag{3.2.3}$$

Si l est impair, alors toutes les solutions positives de l'équation (3.2.2) *sont données par*

$$x = h_{2nl-1}, \quad et \quad y = k_{2nl-1}$$

et celles de l'équation (3.2.3) *par*

$$x = h_{(2n-1)l-1}, \quad et \quad y = k_{(2n-1)l-1}$$

Remarque 3.2.1. En contraste avec le cas $N = 1$ qui admet une infinité des solutions dès que D soit un entier positif qui n'est pas un carré parfait, l'équation de Pell-Fermat négatif n'admet pas toujours des solutions et si elle en admet, les solution sont en nombre infini.

3.2.2 Équation de Pell-Fermat généralisée

Dans cette sous-section nous considérons l'équation de Pell-Fermat généralisée donnée par,

$$U^2 - DV^2 = N. \tag{3.2.4}$$

où N est un entier rationnel donné et D est comme dans le paragraphe précédent positif et sans facteur carré.

Cette équation n'admet pas toujours des solutions, mais que si elle en possède leur nombre est infini. Ici, nous aurons besoin d'autres notions pour caractériser toutes les solutions de l'équation (3.2.4) lorsqu'elles existent.

Soient $u+v\sqrt{D}$ une solution de l'équation (3.2.4) et $x+y\sqrt{D}$ une solution de l'équation

(3.2.4) alors

$$(u + v\sqrt{D})(x + y\sqrt{D}) = (xu + vyD) + (uy + vx)\sqrt{D}$$

et qu'en vertu de l'identité de Brahmagupta, nous avons

$$(xu + vyD)^2 - D(uy + vx)^2 = (u^2 - Dv^2)(x^2 - Dy^2) = N.$$

Ainsi, en posant $u' = xu + vyD$ et $v' = uy + vx$, on remarque alors que $u' + v'\sqrt{D}$ est aussi solution de l'équation (3.2.4).

Définition 3.2.2. *Soient $u + v\sqrt{D}$ et $u' + v'\sqrt{D}$ deux solutions de l'équation* (3.2.4)*. Ces solutions sont dites associées, s'il existe une solution $x + y\sqrt{D}$ de l'équation* (3.2.2)*, tel que*

$$u' + v'\sqrt{D} = (u + v\sqrt{D})(x + y\sqrt{D}).$$

L'ensemble des solutions associées les unes des autres de l'équation (3.2.4) forment une classe K des solutions de cette équation et il est clair, d'après le traitement de l'équation (3.2.2) que la classe K contient une infinité des solutions. On se pose, alors, la question de savoir quand est ce que deux solutions données $u + v\sqrt{D}$ et $u' + v'\sqrt{D}$ sont dans la même classe. Il existe une condition nécessaire et suffisante pour cela. Notamment que

$$\frac{uu' - Dvv'}{N} \in \mathbb{Z} \quad \text{et} \quad \frac{vu' - uv'}{N} \in \mathbb{Z}$$

Soient K la classe des solutions de l'équation (3.2.4) de la forme $u_n + v_n\sqrt{D}$ et K' la classe contenant celles de la forme $u_n - v_n\sqrt{D}$ où $n \in \mathbb{N}$. Alors K et K' sont dites classes conjuguées l'une de l'autre. Lorsque les classes conjuguées coïncident, fait rarissime, alors elles sont dites ambiguës.

Soit K une classe des solutions de l'équation (3.2.4). Parmi ces solutions, on peut choisir une, $u_0 + v_0\sqrt{D}$ par exemple, avec la plus petite valeur positive possible de v_0. Dans le cas où la classe K n'est pas ambigüe, puisque $-u_0 + v_0\sqrt{D}$ est dans la classe conjuguée, u_0 est défini de manière unique aussi, par contre dans la cas ambigüe pour avoir l'unicité on choisit la valeur positive de u_0. La solution déterminée ainsi est appelée la solution fondamentale de la classe de K.

Les théorèmes qui suivent fournissent des bornes que la solution fondamentale d'une classe K doit vérifiée selon que N est positif ou négatif.

Théorème 3.2.3. *Si $u + v\sqrt{D}$ est la solution fondamentale de la classe K de l'équation 2.3.7 et si $x_1 + y_1\sqrt{D}$ est la solution fondamentale de l'équation* (3.2.2)*, nous avons les inégalités*

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1+1)}}\sqrt{N}$$

et

$$0 < |u| \leq \sqrt{\frac{(x_1+1)N}{2}}.$$

Dans le cas où N est négatif nous avons le théorème analogue suivant.

Théorème 3.2.4. *Si $u + v\sqrt{D}$ est la solution fondamentale de la classe K de l'équation* (2.3.7) *avec N négatif et si $x_1 + y_1\sqrt{D}$ est solution la fondamentale de l'équation* (3.2.2)*, nous avons les inégalités*

$$0 \leq v \leq \frac{y_1}{\sqrt{2(x_1-1)}}\sqrt{|N|}$$

et

$$0 < |u| \leq \sqrt{\frac{(x_1-1)|N|}{2}}.$$

Remarque 3.2.2. Les bornes données par les théorèmes précédents sont très efficaces pour déterminer la solution fondamentale d'une classe K quand elles sont petites, cependant elles peuvent devenir facilement gigantesque et rendent pénible voire impossible à la main la détermination de la solution fondamentale d'une classe K.

La caractérisation des toutes les solutions de l'équation de Pell-Fermat généralisée est donnée par le théorème suivant.

Théorème 3.2.5. *Si D est entier positif qui n'est pas un carré parfait et $N \in \mathbb{Z}$, alors l'équation* (3.2.4) *possède un nombre fini des classes de solutions. Les solutions fondamentales de toutes les classes peuvent être déterminées après un nombre fini de tests des inégalités données dans les théorèmes 3.2.3 et 3.2.4.*
Si $u_0 + v_0\sqrt{D}$ est la solution fondamentale de la classe K et $x + y\sqrt{D}$ est une solution de l'équation (3.2.2) *ou* (3.2.3)*, alors toutes les solutions de la classe K sont données par*

$$u_n + v_n\sqrt{D} = (u_0 + v_0\sqrt{D})(x + y\sqrt{D})^n$$

Nous finissons cette section par la remarque suivante.

Remarque 3.2.3.

1) Si l'équation (3.2.4) n'admet aucune solution qui vérifie les inégalités données dans les théorèmes 3.2.3 et 3.2.4 alors elle n'admet pas des solutions.

2) Une condition nécessaire mais non suffisante pour que l'équation (3.2.4) soit résoluble est que N soit un résidu quadratique modulo D.

3.3 Sur l'équation diophantienne de la forme $x^2 - kxy + ky^2 + ly = 0$

Dans cette section nous donnons notre résultat portant sur l'étude de l'équation diophantienne $x^2 - kxy + ky^2 + ly = 0$. Ce résultat est contenu dans Alkabouss et al [2].

3.3.1 Introduction

Des nombreux résultats traitant l'équation diophantienne en question ont été publiés. Par exemple, pour les entiers k et l fixés, Hu et Le [39] ont étudié l'équation diophantienne

$$x^2 - kxy + y^2 + lx = 0. \tag{3.3.1}$$

Pour $l = 1$, Marlewsli et Zarzycki [51] ont montré que cette équation admet une infinité des solutions entières positives si et seulement si $k = 3$. De plus, ils ont posé la question de savoir s'ils existent d'autres valeurs de k pour lesquels l'équation (3.3.1) admet une infinité des solutions entières.

Keskin [44] a étudié l'équation (3.3.1) pour $l = -1$ et $l = 1$. Il a montré que pour $k > 3$, l'équation (3.3.1) avec $l = 1$ n'admet pas des solutions entières positives, mais que pour $l = -1$, elle a une infinité des solutions entières. Il a considéré aussi les équations diophantiennes $x^2 - kxy - y^2 \pm y = 0$ et il a prouvé que ces équations admettent de solutions entières positives pour $k \geq 1$.

Ultérieurement, Yuan et Hu [83] ont répondu positivement à la question de Marlewsli

et Zarzycki [51] en montrant que l'équation (3.3.1) pour $l = 1$, admet un nombre infini des solutions entières si et seulement si $k \neq 0$ et $k \neq \pm 1$. Ils ont aussi considéré l'équation (3.3.1) quand $l = 2$ et $l = 4$ et ont déterminé pour quelles valeurs de l'entier positif k ces équations admettent une infinité de solutions entières positives.

Keskin, Karaatli et Şiar, dans [43] et [42], ont traité les équations

$$x^2 - kxy + y^2 - 2^n = 0 \tag{3.3.2}$$

et

$$x^2 - kxy + y^2 + 2^n = 0 \tag{3.3.3}$$

respectivement. Ils ont déterminé quand est ce qu'elles admettent une infinité de solutions entières positives pour $0 \leq n \leq 10$. Dans le même papiers les auteurs énoncèrent la conjecture suivante :

Conjecture 3.3.1.

(i) Soit n un entier impair et $n > 2$. Si $k > 2^n - 2$ alors l'équation (3.3.2) n'admet pas des solutions entières positives. Si $k \leq 2^n - 2$ et l'équation (3.3.2) admet une solution, alors k est pair.

(ii) Soit n un entier pair. Si $k > 2^n - 2$, alors l'équation (3.3.3) n'admet pas des solutions entières positives impairs. Si $k \leq 2^n - 2$ et l'équation (3.3.3) admet une solution entière positive impaire, alors k est pair.

Karaatli et Şiar [41] ont considéré l'équation diophantienne

$$x^2 - kxy + ky^2 + ly = 0 \tag{3.3.4}$$

pour $l = 2^\kappa, 0 \leq \kappa \leq 3$, et ont déterminé pour quelles valeurs de l'entier positive k, ces équations possèdent une infinité de solutions entières positives.

Recement, Mavecha [52] a considéré l'équation (3.3.4) pour $l = 2^n$, où n est un entier positif ou nul et k un entier impair. Elle a montré que cette équation admet une infinité de solutions entières positives x et y si et seulement si $k = 5$.

Boumahdi et Al, dans [15], ont démontré, entre autres résultats, la conjecture de Keskin et al.

Dans [2], nous avons traité l'équation (3.3.4) où k et l sont des entiers, avec k paire, satisfaisant certaines conditions, que nous déterminons, sous lesquelles cette équation admet une infinité des solutions entières positives. Nous traitons, également, la même équation pour les valeurs $l = 3^n$ et $k \equiv 2 \pmod 3$; $l = 2^r 3^s$ and $k = 2k' + 1$ avec $k' \equiv 2 \pmod 3$ avec n, s, t des entiers positifs. Nos résultats génélarisent ceux de Karaatli et Şiar [41].

3.3.2 L'équation $x^2 - kxy + ky^2 + ly = 0$ avec k pair

Dans cette sous section nous présentons le résultat principal du chapitre. En fait, nous démontrons le théorème suivant.

Théorème 3.3.2. *Soient l et k des entiers avec k pair. Si $l^2 < k$, alors l'équation $x^2 - kxy + ky^2 + ly = 0$ admet un nombre infini des solutions entières positives x et y si et seulement $(l,k) = (2,6)$. De plus, les solutions sont données par les suites (où $x_n = x$ et $y_n = y$)*

$$\begin{cases} x_n &= \dfrac{v_n - u_n}{2} - 1 \\ y_n &= -\dfrac{1}{6}(u_n - 2) \end{cases}$$

où n est un entier impair et u_n, v_n sont donnés par les suites suivantes :

$$\begin{cases} u_n &= -2\left((2)^n + \displaystyle\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (2)^{n-2i} (3)^i\right) \\ v_n &= \pm 2\left(\displaystyle\sum_{i=1}^{\frac{n+1}{2}} \binom{n}{2i-1} (2)^{n-2i+1} (3)^{i-1}\right) \end{cases}$$

Démonstration. Supposons qu'ils existent certains entiers positifs x et y qui vérifient l'équation (3.3.4). En complétant le carré nous obtenons,

$$\left(x - \frac{k}{2}y\right)^2 + \left(k - \frac{k^2}{4}\right)y^2 + ly = 0. \tag{3.3.5}$$

Posons $a = \left(k - \frac{k^2}{4}\right)$. En multipliant la dernière équation par $4a$ nous obtenons l'équation suivante

$$a\left(2x - ky\right)^2 + \left(2ay + l\right)^2 = l^2.$$

Par le changement des variables $u = 2ay + l$ and $v = 2x - ky$, nous avons l'équation

$$u^2 - \left(\frac{k^2}{4} - k\right)v^2 = l^2. \tag{3.3.6}$$

Dans l'équation (3.3.6) si $k = 2$, alors nous obtenons $u^2 + v^2 = l^2$ qui admet un nombre fini de solutions entières en fonction l. Si $k = 4$, nous avons alors $u^2 = l^2$, donc dans ce cas aussi l'équation possède un nombre fini des solution. Ainsi, nous pouvons supposer que $k > 4$, en d'autres termes $\left(\frac{k^2}{4} - k\right) > 0$ et donc nous avons une équation de Pell-Fermat généralisée. La solution fondamentale de l'équation de Pell-Fermat

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

est donnée par $u_1 = \frac{k}{2} - 1$ and $v_1 = 1$.

Soit $u + v\sqrt{\left(\frac{k^2}{4} - k\right)}$ la solution fondamentale de la classe K de l'équation (3.3.6). Par le théorème 3.2.3, nous trouvons que $0 \leq v \leq \frac{l}{\sqrt{k}}$.

Si $\frac{l}{\sqrt{k}} < 1$ alors il y a seulement une classe de solutions dont la solution fondamentale est donnée par $v = 0$ et $u = \pm l$. Le nombre infini de solutions entières de cette classe peut être trouvé à partir de la formule

$$u_n + v_n\sqrt{\frac{k^2}{4} - k} = \pm l\left(\frac{k}{2} - 1 + \sqrt{\frac{k^2}{4} - k}\right)^n.$$

Alors u_n et v_n sont donnés comme suit.

$$\begin{cases} u_n = & \pm l\left(\left(\frac{k}{2}-1\right)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i}\left(\frac{k}{2}-1\right)^{n-2i}\left(\frac{k^2}{4}-k\right)^i\right) \\ v_n = & \pm l\left(\sum_{i=1}^{\lfloor \frac{n+1}{2} \rfloor} \binom{n}{2i-1}\left(\frac{k}{2}-1\right)^{n-2i+1}\left(\frac{k^2}{4}-k\right)^{i-1}\right) \end{cases}$$

Les solutions de l'équation (3.3.4) sont données par

$$\begin{cases} 2x_n - ky_n & = v_n \\ -2\left(\frac{k^2}{4}-k\right)y_n + l & = u_n \end{cases}$$

Comme $k > 4$, nous avons $\left(\frac{k^2}{4}-k\right) > k > l^2$ et comme $y_n \geq 1$ (parce que nous sommes intéressées par de solutions entières positives seulement) alors $u_n < 0$. Donc à partir de maintenant, nous considérons que u_n est négatif. En prenant les équations des deux systèmes précédents modulo $\left(\frac{k}{2}-2\right)$ nous obtenons que $u_n \equiv -l \left(mod\, \frac{k}{2}-2\right)$ et $u_n \equiv l \left(mod\, \frac{k}{2}-2\right)$. Autrement dit, nous avons $2l \equiv 0 \left(mod\, \frac{k}{2}-2\right)$, ainsi $k-4$ divise $4l$. Comme $l^2 - 4 < k - 4 \leq 4l$, nous avons $l^2 - 4l - 4 < 0$ et donc

$$l \in \{1,2,3,4\}$$

.

Dans la suite, nous déterminons pour chaque valeur de l, dans la liste précédente, les valeurs de k correspondantes, si elles existent, pour lesquelles l'équation (3.3.4) admet une infinité de solutions entières positives.

1) Si $l = 1$ d'après ce qui précède 4 est un multiple de $k-4$ et $k > 1$. Ainsi $k \in \{5,6,8\}$ et comme nous nous intéressons qu'aux valeurs paires de k seulement, alors $k \in \{6,8\}$. Pour ces valeurs de k,il n'existe aucune solution entière positive à l'équation (3.3.4) en considérant certaines congruences convenables comme nous le verrons.

- Pour k=6, d'après ce qui précède, nous avons les équations suivantes :

$$u_n = -\left((2)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (2)^{n-2i} (3)^i\right) \tag{3.3.7}$$

$$-6y_n + 1 = u_n. \tag{3.3.8}$$

De l'équation (3.3.8), nous avons $u_n \equiv 1\,(mod\,2)$, alors que l'équation (3.3.7) donne $u_n \equiv 0\,(mod\,2)$. D'où la contradiction.

- Pour $k = 8$, nous obtenons les équations suivantes :

$$u_n = -\left((3)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (3)^{n-2i} (8)^i\right) \tag{3.3.9}$$

$$-16y_n + 1 = u_n. \tag{3.3.10}$$

En considérant l'équation (3.3.10) modulo 8, nous obtenons $u_n \equiv 1\,(mod\,8)$. L'équation (3.3.9) modulo 8 donne $u_n \equiv -1\,(mod\,8)$ pour n pair et $u_n \equiv -3\,(mod\,8)$ pour n impair, ce qui contredit la première congruence.

2) Si $l = 2$ alors $k-4$ divise 8, donc $k \in \{5,6,8,12\}$ et comme k doit être pair et $k > 4$, donc $k \in \{6,8,12\}$.

- Pour k=6, d'après ci dessus-ci, nous avons :

$$u_n = -2\left((2)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (2)^{n-2i} (3)^i\right) \tag{3.3.11}$$

$$-6y_n + 2 = u_n. \tag{3.3.12}$$

Considérons (3.3.12) modulo 3, nous trouvons que $u_n \equiv 2\,(mod\,3)$. De l'équation (3.3.11), pour n pair nous trouvons que $u_n \equiv -2\,(mod\,8)$ d'où la contradiction. A partir de l'équation (3.3.12), nous voyons que y_n existe si et seulement si 3 divise $(u_n - 2)$, qui est en accord avec l'équation (3.3.11) car $u_n \equiv$

$-1\,(mod\,3)$ pour n impair. En examinant le système suivant pour x_n,

$$\begin{cases} 2x_n - 6y_n &= v_n \\ -6y_n + 2 &= u_n \end{cases}$$

nous apercevons que

$$2x_n - 2 = v_n - u_n \Leftrightarrow x_n - 1 = \frac{v_n - u_n}{2}.$$

Donc x_n existe si et seulement si u_n et v_n sont de la même parité. Ce qui est évidement vrai. Ainsi, dans ce cas nous avons une infinité de solutions entières positives et celles ci sont données par

$$\begin{cases} x_n = & \frac{v_n - u_n}{2} + 1 \\ y_n = & -\frac{1}{6}(u_n - 2) \end{cases}$$

- Pour $k = 8$, nous avons les équations suivantes

$$u_n = -2\left((3)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (3)^{n-2i} (8)^i\right) \tag{3.3.13}$$

$$-16y_n + 2 = u_n. \tag{3.3.14}$$

L'équation (3.3.14) donne $u_n \equiv 2\,(mod\,8)$ et $u_n \equiv 2\,(mod\,8)$, tandis que l'équation (3.3.13) donne, pour n pair , $u_n \equiv -2 \pmod 8$, et pour n impair, $u_n \equiv -6 \pmod 8$, ce qui donne une contradiction.

- Pour $k = 12$, nous obtenons les équations suivantes.

$$u_n = -2\left((5)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (5)^{n-2i} (24)^i\right) \tag{3.3.15}$$

$$-48y_n + 2 = u_n. \tag{3.3.16}$$

De l'équation (3.3.16), nous apercevons que $u_n \equiv 2\,(mod\,24)$, alors que l'équation (3.3.15) nous donne $u_n \equiv -2\,(mod\,24)$ pour n pair et $u_n \equiv -10\,(mod\,24)$

pour n impair, ce qui est absurde.

3) Si $l = 3$ alors 12 est un multiple de $k-4$, et donc $k \in \{5,6,7,8,10,16\}$. Puis que, nous somme intéressés en les valeurs de k pair et $k > 9$, alors nous vérifierons les valeurs qui sont dans l'ensemble $\{10,16\}$
   - Pour $k = 10$, nous avons les équations suivantes

$$u_n = -3\left((4)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (4)^{n-2i} (15)^i\right) \tag{3.3.17}$$

$$-30y_n + 3 = u_n. \tag{3.3.18}$$

   A partir de l'équation (3.3.18), nous obtenons $u_n \equiv 3\,(mod\,15)$ et $u_n \equiv 3\,(mod\,30)$, tandis que l'équation (3.3.17) donne $u_n \equiv -3\,(mod\,15)$ pour n pair et $u_n \equiv -12\,(mod\,30)$ pour n impair, ce qui est impossible
   - Pour $k = 16$, nous avons les équations suivantes

$$u_n = -3\left((7)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (7)^{n-2i} (48)^i\right) \tag{3.3.19}$$

$$-96y_n + 3 = u_n. \tag{3.3.20}$$

   En considérant l'équation (3.3.20) modulo 48, nous obtenons $u_n \equiv 3\,(mod\,48)$, mais l'équation (3.3.19) donne $u_n \equiv -21\,(mod\,48)$ pour n pair et $u_n \equiv -3\,(mod\,48)$ pour n impair, ce qui est absurde.

4) Si $l = 4$ alors 16 est multiple de $k-4$, et donc $k \in \{5,6,8,12,20\}$, mais comme k doit être pair et $k > 16$, alors la seule valeur de k à vérifier est $k = 20$.
   - Pour $k = 20$, nous obtenons les équations suivantes

$$u_n = -4\left((9)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (9)^{n-2i} (80)^i\right) \tag{3.3.21}$$

$$-160y_n + 4 = u_n. \tag{3.3.22}$$

Considérant l'équation (3.3.22) modulo 80, nous remarquons que $u_n \equiv 4\,(mod\,80)$. Nous obtenons de l'équation (3.3.21) que $u_n \equiv -36\,(mod\,80)$ si n est impair, et pour n pair que $u_n \equiv -4\,(mod\,80)$. Dans tous les cas nous trouvons une contradiction.

□

Nous déduirons dans le corollaire suivant le Théorème 3.1, le Théorème 3.2 et le Théorème 3.3 de Karaatli et Şiar [41] et nous les rendrons beaucoup plus précis.

Corollaire 3.3.3.

(i) L'équation $x^2 - kxy + ky^2 + y = 0$ admet une infinité de solutions entières positives x et y si et seulement $k = 5$.

(ii) L'équation $x^2 - kxy + ky^2 + 2y = 0$ admet une infinité de solutions entières positives x et y si et seulement $k = 6, 5$.

(iii) L'équation $x^2 - kxy + ky^2 + 4y = 0$ admet une infinité de solutions entières positives x et y si et seulement $k = 5, 6, 8$.

Démonstration.

(i) Mavecha [52] a démontré que la seule valeur impaire de k pour laquelle il existe une infinité des solutions entières positives x et y de l'équation (3.3.4) est $k = 5$. En vue du théorème précédent, il reste à considérer le cas k pair et $k \leq 1$. Donc il y en a aucun.

(ii) Le cas k impair est fait par Mavecha [52]. Nous avons démontré que quand k est pair et $l^2 < k$ alors la seule valeur de k pour laquelle il existe une infinité des solutions entières positives x et y l'équation (3.3.4) est $k = 6$. Donc, il reste à traiter le cas $k \leq l^2$ et k pair. Autrement dit, $k \leq 4$. Mais ces valeurs de k ont été traité avant l'énoncé du théorème.

(iii) Comme ci-dessus , nous rappelons qu'il a été prouvé par Mavecha [52] que $k = 5$ est la seule valeur impaire de k tel que l'équation (3.3.4) admet une infinité des solutions entières x et y. En vue de notre théorème, il reste à considérer le cas k pair où $4 < k \leq 16$. Ainsi nous allons traiter les valeurs de k dans l'ensemble suivant $k \in \{6, 8, 10, 12, 16\}$.

- Pour $k = 6$, nous obtenons les équations suivantes

$$u_n = -4\left((2)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (2)^{n-2i} (3)^i\right) \tag{3.3.23}$$

$$-6y_n + 4 = u_n. \tag{3.3.24}$$

Nous avons d'après l'équation (3.3.24) que $u_n \equiv 1\,(mod\,3)$ et l'équation (3.3.23) donne $u_n \equiv -1\,(mod\,3)$ pour n pair, ce qui est impossible. Pour n impair, de $u_n = -2(3y_n - 2)$ nous apercevons que y_n existe si et seulement si

$$(2^{n+1} + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (2)^{n-2i} (3)^i) \equiv 1\,(mod\,3)$$

ce qui est vrai. Nous avons, aussi, que x_n existe si et seulement si u_n et v_n sont pairs, ce qui est vrai aussi. Donc dans ce cas, nous avons une infinité de solutions entières positives données par

$$\begin{cases} x_n = & \dfrac{v_n - u_n}{2} + 2 \\ y_n = & -\dfrac{1}{6}(u_n - 4) \end{cases}$$

- Pour $k = 8$, les équations que nous obtenons sont les suivantes

$$u_n = -4\left((3)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (3)^{n-2i} (8)^i\right) \tag{3.3.25}$$

$$-16y_n + 4 = u_n. \tag{3.3.26}$$

En considérant l'équation (3.3.26) modulo 16 nous obtenons alors $u_n \equiv 4\,(mod\,16)$, mais l'équation (3.3.25) donne $u_n \equiv -4\,(mod\,16)$ pour n pair, par conséquent nous avons une contradiction. Pour n impair, pour que y_n existe, il est nécessaire et suffisant que $(u_n - 4) \equiv 0$ (mod 16) qui est vérifié dans l'équation (3.3.25). Aussi, d'après le

système des équations suivant

$$\begin{cases} 2x_n - 8y_n & = v_n \\ -16y_n + 4 & = u_n \end{cases}$$

nous avons $4x_n = 2v_n - (u_n - 4)$, donc x_n existe si et seulement si v_n est pair, qui est vrai aussi. Par conséquent, dans ce cas également nous avons une infinité de solutions entières positives données par

$$\begin{cases} x_n = & \dfrac{2v_n - u_n}{4} + 1 \\ y_n = & -\dfrac{1}{16}(u_n - 4) \end{cases}$$

- Pour $k = 10$, nous avons les équations qui suivent

$$u_n = -4\left((4)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (4)^{n-2i} (15)^i\right) \tag{3.3.27}$$

$$-30y_n + 4 = u_n. \tag{3.3.28}$$

En prenant l'équation (3.3.28) modulo 30 nous avons $u_n \equiv 4\,(mod\,30)$ et de l'équation (3.3.27) nous avons que $u_n \equiv -4\,(mod\,30)$, pour n pair, et $u_n \equiv -16\,(mod\,30)$ pour n impair, d'où la contradiction.

- Pour $k = 12$, nous obtenons les équations suivantes

$$u_n = -4\left((5)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (5)^{n-2i} (24)^i\right) \tag{3.3.29}$$

$$-48y_n + 4 = u_n. \tag{3.3.30}$$

En considérant modulo 48 l'équation (3.3.30), nous trouvons alors $u_n \equiv 4\,(mod\,48)$. Alors que, nous obtenons de l'équation (3.3.29) que $u_n \equiv -4\,(mod\,48)$ pour n pair et $u_n \equiv -20\,(mod\,48)$ pour n impair. ce qui est impossible.

- For $k = 16$, nous obtenons les équations suivantes

$$u_n = -4\left((7)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} (7)^{n-2i} (48)^i\right) \tag{3.3.31}$$

$$-96y_n + 4 = u_n. \tag{3.3.32}$$

L'équation (3.3.32) modulo 48 donne $u_n \equiv 4\,(mod\,48)$. Tandis que nous obtenons de l'équation (3.3.31) que $u_n \equiv -4\,(mod\,48)$ pour n pair et $u_n \equiv -28\,(mod\,48)$ pour n impair. Ce qui est absurde.

Ce qui achève la démonstration et donc les seules valeurs de k pour lesquelles l'équation (3.3.4) admet une infinité des solutions entières positives x et y sont $k = 5, 6, 8$. □

Remarque 3.3.1. Nous n'avons pas traité le cas $l = 8$ dans le Théorème 3.3.2. Ce cas correspond au Théorème 3.4 dans Karaatli et Şiar[41]. Cependant, nous pouvons dire, en vue de notre théorème principal et du résultat de Mavecha [52], qu'il reste à traiter le cas k pair où $k \leq 64$. Donc nous devons traiter 32 équations où l et k sont connus. Toutes ces équations peuvent être traitées de la même manière, donc nous traitons le cas $l = 8$ et $k = 8$ comme exemple. Dans ce cas l'équation est donnée par

$$x^2 - 8xy + 8y^2 + 8y = 0.$$

D'après ce qui précède , nous obtenons l'équation de Pell-Fermat généralisée

$$u^2 - 8v^2 = 64.$$

La solution fondamentale de l'équation de Pell-Fermat $u^2 - 8v^2 = 1$ est $u_1 = 3$ and $v_1 = 1$. Par le théorème 3.2.3 nous trouvons que $0 \leq v \leq 1$. Ainsi, $v \in \{0, 1, \}$, mais $v = 1$ ne vérifie pas l'équation de Pell-Fermat généralisée. Ainsi, il y a une seule classe ambiguë des solutions donnée par $v = 0$, et $u = \pm 8$. Le nombre infini des solutions de cette classe peut être obtenu à partir de la formule

$$u_n + \sqrt{8}v_n = \pm 8\left(3 + \sqrt{8}\right)^n.$$

Par les mécanismes développés au cours de la preuve du Théorème 3.3.2, nous obtenons le système des équations suivant

$$\begin{cases} u_n = & -8\left((3)^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i}(3)^{n-2i}(8)^i\right) \\ v_n = & \pm 8\left(\sum_{i=1}^{\lfloor \frac{n+1}{2} \rfloor} \binom{n}{2i-1}(3)^{n-2i+1}(8)^{i-1}\right) \end{cases}$$

et

$$\begin{cases} 2x_n - 8y_n & = v_n \\ -16y_n + 8 & = u_n \end{cases}$$

Nous remarquons de ce système que u_n est négatif. En analysant ces deux systèmes, nous apercevons que y_n existe si et seulement si $u_n - 8 \equiv 0 \,(mod\, 16)$ ce qui est vérifié et pour x_n d'exister, de l'équation $4x_n - 8 = 2v_n - u_n$, nous devons avoir que u_n et v_n soient pairs, ce qui est vrai aussi. Alors dans ce cas nous avons une infinité de solutions entières positives x et y à l'équation (3.3.4) donnée par les suites suivantres

$$\begin{cases} x_n = & \frac{2v_n - u_n}{4} + 2 \\ y_n = & -\frac{1}{16}(u_n - 8) \end{cases}.$$

Cela est en accord avec le Théorème 3.4 dans Karaatli et Şiar [41].

Remarque 3.3.2. Pour traiter le cas $l = 2^4$, de notre Théorème 3.3.2 et Mavecha [52], il reste à traiter le cas k pair et $k \leq 2^8$. Donc pour chaque valeur de l nous avons une borne sur k et qu'il y a un nombre fini des équations à résoudre. Puisqu'il ne reste que des calculs et que tous ceux ci peuvent être traités comme dans la remarque précédente, nous les avons omis.

3.3.3 L'équation $x^2 - kxy + ky^2 + ly = 0$ avec $l = 3^n$ et $k \equiv 2 \,(mod\, 3)$

Dans cette partie, nous traitons l'équation (3.3.4) quand $l = 3^n$ et $k \equiv 2 \,(mod\, 3)$ où n est un entier positif. Pour ces valeurs de k et l nous avons le théorème suivant.

Théorème 3.3.4. *l'équation $x^2 - kxy + ky^2 + ly = 0$, où $l = 3^n$ et $k \equiv 2 \,(mod\, 3)$ sont des*

entiers et n un entier positif ou nul, admet une infinité de solutions entières positives x et y si et seulement $k = 5$.

Avant de donner la démonstration de ce théorème, nous donnons deux lemmes de Mavecha [52] qui seront utilisés dans la preuve.

Lemme 3.3.5. *L'équation (3.3.4) admet une solution si et seulement si l'équation*

$$X^2 - kXY + kY^2 + LY = 0$$

admet une solution pour un certain entier L avec $L|l$ et $pgcd(Y, L) = 1$.

Lemme 3.3.6. *Si (x, y) est une solution de (3.3.4) avec $pgcd(y, l) = 1$, alors y est un carré.*

Nous donnons maintenant la preuve du théorème précédent

Démonstration. Nous divisons la démonstration en deux cas.

1. Supposons d'abord que $n > 0$. Soit (x, y) une solution de l'équation (3.3.4), alors le Lemme 3.3.5 affirme que nous pouvons supposer $pgcd(y, l) = 1$. Dans ce cas, d'après le Lemma 3.3.6 y est un carré. Posons $y = \alpha^2$, et donc de l'équation (3.3.4) nous obtenons que $x = \alpha t$. Ainsi, l'équation (3.3.4) devient

$$t^2 - k\alpha t + k\alpha^2 + 3^n = 0. \tag{3.3.33}$$

   Nous considerons les points suivants :
   (i) Si $3|t$, comme $pgcd(y, l) = pgcd(\alpha^2, 3^n) = 1$, en considérant l'équation (3.3.33) modulo 3, nous apercevons que $k \equiv 0\,(mod\,3)$ qui contredit l'hypothèse que $k \equiv 2\,(mod\,3)$.
   (ii) Si $3 \nmid t$, alors en considérant l'équation (3.3.33) modulo 3, nous trouvons que $-k\alpha t \equiv 0\,(mod\,3)$. Nous obtenons encore une contradiction, car aucun de ces entiers n'est divisible par 3.

2. Supposons maintenant que $n = 0$. Dans ce cas, l'éequation (3.3.4) devient $x^2 - kxy + ky^2 + y = 0$. Mais cette dernière équation est traitée dans le Théorème 3.1 de Karaatli et Şiar [41] où il est démontré que l'équation (3.3.4) admet une infinité de solutions entières positives si et seulement si $k = 5$.

□

3.3.4 L'équation $x^2 - kxy + ky^2 + ly = 0$ avec $l = 2^r 3^s$ et $k = 2k' + 1$ avec $k' \equiv 2\,(mod\,3)$

Nous avons aussi traité l'équation (3.3.4) pour $l = 2^r 3^s$ et $k = 2k' + 1$ avec $k' \equiv 2\,(mod\,3)$ où s, t sont des entiers positifs. Pour ces valeurs de k et l nous avons le théorème suivant.

Théorème 3.3.7. *L'équation $x^2 - kxy + ky^2 + ly = 0$, pour $l = 2^r 3^s$ et $k = 2k' + 1$ avec $k' \equiv 2\,(mod\,3)$ des entiers où s, t sont des entiers positifs ou nuls, admet une infinité de solutions entières positives x et y si et seulement $k = 5$.*

Démonstration. Nous suivons les mêmes étapes que dans la démonstration du théorème précédent.

1) Supposons, d'abord, que $r > 0$ et $s > 0$. Soit (x, y) une solution de l'équation (3.3.4), alors le Lemme 3.3.5 affirme que nous pouvons supposer $pgcd(y, l) = 1$. Dans ce cas, d'après le Lemma 3.3.6 y est un carré. Posons $y = \alpha^2$, et donc de l'équation (3.3.4) nous obtenons que $x = \alpha t$. Ainsi, l'équation (3.3.4) devient

$$t^2 - k\alpha t + k\alpha^2 + 2^r 3^s = 0. \tag{3.3.34}$$

Nous considérons les points suivants.

(i) Si $3|t$, comme $pgcd(y, l) = pgcd(\alpha^2, 2^r 3^s) = 1$, en considérant l'équation (3.3.34) modulo 3, nous apercevons que $k \equiv 0\,(mod\,3)$ qui contredit notre hypothèse selon laquelle $k' \equiv 2\,(mod\,3)$.

(ii) Si $3 \nmid t$, en considérant, également, l'équation (3.3.34) modulo 3, nous obtenons que $-k\alpha t \equiv 0\,(mod\,3)$. D'où la contradiction, car aucun de ces entiers n'est divisible par3.

2) Si $r = 0$ et $s \neq 0$ nous obtenons le théorème précédent et si $r \neq 0$ et $s = 0$ nous obtenons le Théoréme 2.3 dans Mavecha [52]. Donc il reste à traiter le cas $r = s = 0$. Dans ce cas aussi, l'équation (3.3.4) devient $x^2 - kxy + ky^2 + y = 0$ qui est traité dans le Théorème 3.1 de Kaartli et Şiar [41] où il est démontré que l'équation (3.3.4) admet une infinité de solutions entières positives si et seulement si $k = 5$.

□

Chapitre 4

Formes quadratiques et nombre des classes

L'objectif de ce présent chapitre est l'étude de la décomposition des nombres premiers dans certains corps quadratiques imaginaires. Pour le besoin de cet objectif, le rappel de certains concepts liés au nombre des classes des corps quadratiques en question est nécessaire. Ainsi le chapitre est subdivisé en trois parties. Dans la première section nous présentons quelques notions générales sur les formes quadratiques binaires entières, la deuxième section est consacrée à quelques rappels de la théorie algébrique de nombres et enfin dans la troisième section nous donnons notre résultat qui porte sur une borne inférieure concernant les nombres premiers qui se décomposent dans un corps quadratique imaginaire en fonction du nombre des classes de ce corps.

4.1 Formes quadratiques

La théorie des formes quadratiques binaires entières a joué un rôle majeur dans le développement de la théorie des nombres moderne. La théorie peut être remontée à Fermat à travers son fameux théorème sur la somme de deux carrés et d'autres théorèmes du même genre qui ont été démontré plus tard par Euler. Cela a permis à Euler de découvrir la loi de réciprocité quadratique et de conjecturer d'autres résultats dans la même direction. Ultérieurement, Lagrange a développé la théorie générale

des formes quadratiques binaires pour traiter le problème des représentations des entiers par ces formes, en introduisant les notions de discriminants, des substitutions linéaires, d'équivalences de formes, des formes quadratiques binaires réduites. Legendre et plus tard Gauss ont introduit la composition des deux formes. Gauss a démontré la loi de réciprocité quadratique. Il a démontré, également, que les classes des formes quadratiques binaires primitives définies positive de discriminant fixé forment un groupe fini dont la loi de composition est donnée par la composition des formes quadratiques.
Dans le sens de Lagrange, une forme quadratique binaire entière est donnée par

$$ax^2 + bxy + cy^2 \qquad (a, b, c \in \mathbb{Z}) \tag{4.1.1}$$

dont le discriminant est $D = b^2 - 4ac$. La définition de Gauss est légèrement différente de celle de Lagrange. Elle est donnée par $a^2 + 2bxy + cy^2$ dont le discriminant est $D = b^2 - ac$. Le signe de D est très important dans l'étude des formes quadratiques. Si $D > 0$ alors la forme peut représenter à la fois les entiers positifs et négatifs, ainsi elle est dite indéfinie. Si $D < 0$, elle représente seulement les entiers positifs ou négatifs selon le signe de a. Elle est dite définie positive si a est positif et définie négative si a est négatif. De la définition du discriminant on tire le théorème suivant qui donne quels entiers rationnels peuvent être discriminant d'une forme quadratique.

Théorème 4.1.1. *Soit D un entier fixé. Il existe au moins une forme quadratique binaire entière de discriminant D si et seulement si $D \equiv 0$ ou 1 (mod 4).*

Dans la suite, nous nous intéresserons seulement aux formes quadratiques définies positives et nous dirons que la forme quadratique est primitive si et seulement si le plus grand commun diviseur de ses coefficient est égale à 1.
On dit qu'un entier m est représenté par la forme $ax^2 + bxy + cy^2$ s'ils existent des entiers x et y tel que

$$m = ax^2 + bxy + cy^2 \qquad (a, b, c \in \mathbb{Z}).$$

La représentation est dite propre si x et y sont premiers entre eux.

Théorème 4.1.2. *Soit m un entier donné non nul. Alors m est proprement représenté par une forme quadratique de discriminant D si et seulement si D est un résidu quadratique*

modulo $|m|$

Deux formes $f(x,y)$ et $f'(x,y)$ sont dite équivalentes s'ils existent des entiers α, β, γ et δ tels que

$$f(x,y) = f'(\alpha x + \beta y, \gamma x + \delta y)$$

et $\alpha\delta - \gamma\beta = \pm 1$. L'équivalence est dite propre si $\alpha\delta - \gamma\beta = 1$. Il est claire que cette équivalence est une relation d'équivalence. Il est facile de voir que les formes quadratiques équivalentes représentent les mêmes nombres. Il est aussi, important de noter que les formes quadratiques équivalentes ont le même discriminant.
La définition qui suit est importante, car elle nous fournit un type particulier et essentiel des formes quadratiques.

Définition 4.1.1. *Une forme quadratique primitive définie positive* $f(x,y) = ax^2 + bxy + cy^2$ *est réduite si* $-a < b \leq a < c$ *ou* $0 \leq b \leq a = c$.

Nous aurons besoin de deux lemmes suivants dans la suite dont les preuves peuvent être trouvées dans Cox [19].

Lemme 4.1.3. *Soit* $F(X,Y) = AX^2 + BXY + CY^2$ *une forme quadratique binaire primitive définie positive qui est réduite. Alors* $F(X,Y) \geq (A - |B| + C)\min(X^2, Y^2)$.

Lemme 4.1.4. *Soit* $F(X,Y) = AX^2 + BXY + CY^2$ *une forme quadratique binaire primitive définie positive qui est réduite de discriminant* $D < 0$ *alors* $A \leq \sqrt{\dfrac{|D|}{3}}$.

Nous dirons que deux formes quadratiques sont dans la même classe si et seulement si elles sont proprement équivalente.

Définition 4.1.2. *Soit* D *un entier donné qui n'est pas un carré parfait. On appelle nombre de classes de* D *le nombre de classes d'équivalences de formes quadratiques binaires de discriminant* D.

Théorème 4.1.5. *Soit* D *un entier donné, qui n'est pas un carré parfait. Toute classe d'équivalence de formes quadratiques binaires de discriminant* D *contient au moins une forme réduite.*

Un autre résultat important dans la théorie des formes quadratiques est le théorème suivant :

Théorème 4.1.6. *Toute forme quadratique définie positive primitive est proprement équivalente à une unique forme réduite.*

Démonstration. Voire Cox [19]. □

Puisque les formes quadratiques binaires que nous considérons seront réduites et que pour un discriminant $D < 0$ fixé, nous avons d'après le Lemme 4.1.4 et le Théorème4.1.6 le théorème suivant :

Théorème 4.1.7. *Soit $D < 0$ un entier donné. Alors le nombre $h(D)$ des classes de formes quadratiques binaires primitives définies positive de discriminant D est fini et il est égal au nombre des formes réduites de discriminant D.*

Soient $f(x,y)$ et $g(x,y)$ deux formes quadratiques primitives définies positives de discriminant D. Une forme quadratique $F(x,y)$ avec le même qualificatif est leur composition si

$$f(x,y)g(u,v) = F(B_1(x,y;u,v), B_2(x,y;u,v))$$

où les

$$B_i(x,y;u,v) = a_i xu + b_i xv + c_i yu + d_i yv \quad \text{pour} \quad i = 1,2$$

sont des formes bilinéaires entières.

Remarque 4.1.1. Il existe plusieurs manières de composer deux formes quadratiques et les formes obtenues ne sont pas nécessairement proprement équivalentes. Pour obtenir une opération bien définie Gauss imposait les conditions suivantes :

$$a_1 b_2 - a_2 b_1 = \pm f(1,0), \quad a_1 c_2 - a_2 c_1 = \pm g(1,0)$$

et définit la notion de composition directe si le signe + survient toujours dans les deux expressions précédentes.

Gauss a démontré le résultat suivant sur la composition de formes quadratiques.

Théorème 4.1.8 (Gauss)**.** *L'ensemble de classes d'équivalences de formes quadratiques binaires muni de la composition directe est un groupe abélien fini.*

Remarque 4.1.2. Il est reconnu, unanimement, que ce résultat est l'une des découvertes la plus profonde de Gauss et a été précurseur à la théorie des groupes qui est née quelques années plus tard.

Récemment, Bhargava [13] a généralisé la loi de composition de Gauss de la manière suivante : Étant donné un cube de sommets entiers, il définit les formes quadratiques à partir de trois paires des faces opposées. Si les nombres sur les deux faces sont placés dans l'ordre dans deux Matrice carrés A et B (ou le même coin est toujours utilisé pour l'entrée droite de A) alors il définit la forme quadratique binaire par le négatif du déterminant de $Ax + By$. Bhargava a démontré que ces trois formes ont le même discriminant et que leur produit est l'identité dans le groupe de classes. De plus, trois formes quadratiques quelconques dont leur produit est l'identité découle de cette manière. De ce résultat Bhargava a obtenu des nombreux résultats profonds en géométrie arithmétique.
Durant le développement de la théorie algébrique des nombres (voir la prochaine section) au dix-neuvième siècle, l'étude des formes quadratiques a été interprété dans cette théorie. Pour une forme quadratique donnée $f(x,y) = ax^2 + bxy + cy^2$ de discriminant D, il peut lui être associée un idéal $(a, \frac{-b+\sqrt{D}}{2})$ qui est un $\mathbb{Z}-$module dans le corps quadratique $\mathbb{Q}(\sqrt{D})$. Deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ sont dit équivalents s'ils différent par un idéal principal, en d'autre termes si ils sont dans la même classe dans le groupe des classes d'idéaux dans l'anneau des entiers $\mathfrak{O}_{\mathbb{Q}(\sqrt{D})}$ de $\mathbb{Q}(\sqrt{D})$. Réciproquement, dans chaque $\mathbb{Z}-$module du corps quadratique $\mathbb{Q}(\sqrt{D})$, en considérant un idéal inversible et en utilisant sa norme on peut lui associer une forme quadratique binaire entière.
Un des faits importants qui lie les deux théories est que l'équivalence des idéaux qu'on vient de définir correspond à l'équivalence des formes quadratiques binaires définies plus haut.

4.2 Quelques notions de la théorie algébrique des nombres

La théorie algébrique des nombres est la branche de la théorie des nombres qui utilise les méthodes algébriques pour résoudre des problèmes liés au nombre. Son développement s'est accéléré au début du vingtième siècle suite aux travaux de Gauss sur les

formes quadratiques et surtout grâce aux tentatives de Kummer sur la résolution du dernier "théorème" de Fermat. En effet, Kummer a introduit la notion des *nombres idéaux* pour compenser le manque des nombres premiers qui font défaut, selon lui, pour obtenir l'unicité de la factorisation des nombres en produit des nombres premiers dans certains anneaux des entiers. Par la suite, Dedekind a généralisé le concept en introduisant les *idéaux*, et a obtenu l'équivalent du *théorème fondamentale de l'arithmétique* dans certains anneaux qui porte son nom de nos jours. Dans cette section nous rappelons certains définitions et résultats, de la théorie, tirés presque entièrement de Marcus [50], Samuel [65], Lang [46], et Niven [59] pour ne citer que ceux là. Nous ne donnons aucune preuve de ces résultats qui peuvent être trouvés dans les livres ci-mentionnés.

4.2.1 Corps de nombres et l'anneau de ses entiers

Nous entendons par *anneau* (respectivement *corps*) dans ce chapitre un *anneau* (respectivement *corps*) *commutatif unitaire*.

Quelques critères d'irréductibilités

Il est connu que si $\mathbb{K}$ est un corps alors l'anneau des polynômes $\mathbb{K}[X]$ est euclidien, en d'autres termes nous avons dans cet anneau la notion de division euclidien, de la factorisation unique en élément irréductible et la notion du plus grand commun diviseur.

Définition 4.2.1. *Un polynôme $f(x)$, non identiquement nul, est irréductible ou premier sur le corps de rationnels $\mathbb{Q}$ s'il ne peut pas s'écrire comme produit $f(x) = g(x)h(x)$ où $g(x)$ et $h(x)$ sont deux polynômes de degrés positifs.*

Définition 4.2.2. *Un polynôme $f(x) = a_n x^n + \cdots + a_0$, à coefficients entiers est dit primitif si le plus grand commun diviseur de ses coefficients est* 1.

Théorème 4.2.1. *Le produit de deux polynômes primitifs est primitif.*

Théorème 4.2.2 (Lemme de Gauss)**.** *Supposons qu'un polynôme unitaire $f(x)$ à coefficients entiers se factorise en deux polynômes unitaires à coefficients rationnels, $f(x) = g(x)h(x)$, alors $g(x)$ et $h(x)$ sont à coefficients entiers.*

Le critère d'Eisenstein permet de savoir quand est ce qu'un polynôme à coefficients dans $\mathbb{Q}$. Il est très pratique dans certains cas.

Théorème 4.2.3 (Critère d'Eisenstein)**.** *Considérons un polynôme $f(x) = a_n x^n + \cdots + a_0$ à coefficients entiers. Si un nombre premier p divise tous les a_i sauf pour $i = n$ et p^2 ne divise pas a_0 alors $f(x)$ est irréductible dans le corps $\mathbb{Q}$ de rationnels.*

Nombres algébriques et entiers algébriques

Définition 4.2.3. *Un nombre complexe α est dit nombre algébrique s'il est solution d'une équation polynomiale $f(x) = 0$ où f est à coefficient dans $\mathbb{Q}$.*

Un nombre complexe qui n'est pas algébrique est dit *transcendant.*

Remarque 4.2.1. Si le coefficient dominant a_n de $f(x)$ est différent de 0, alors il admet un inverse dans $\mathbb{Q}$, on peut donc considérer le polynôme, dans la définition précédente, unitaire. Ainsi, un nombre algébrique α satisfait un unique polynôme unitaire irréductible sur $\mathbb{Q}$.

Définition 4.2.4. *Le polynôme minimal de α est l'unique polynôme unitaire irréductible $f(x)$ tel que $f(x) = 0$. Le degré de $f(x)$ est appelé le degré du nombre algébrique α*

Définition 4.2.5. *Un nombre algébrique α est dit entier algébrique s'il satisfait une équation polynômiale $g(x) = x^n + a_{n-1}x^{n-1} \cdots + a_0$ où les coefficients a_i sont entiers relatifs.*

Théorème 4.2.4. *le polynôme minimal d'un entier algébrique est unitaire est à coefficients entiers.*

Théorème 4.2.5. *Si α et β sont des nombres algébriques, alors $\alpha + \beta$ et $\alpha\beta$ sont aussi des nombres algébriques. Si α et β sont des entiers algébriques, alors $\alpha + \beta$ et $\alpha\beta$ sont aussi des entiers algébriques*

Du théorème précédent, on obtient ce théorème suivant :

Théorème 4.2.6. *L'ensemble de tous les nombres algébrique forment un corps. L'ensemble de tous les entiers algébriques forment un anneau.*

Remarque 4.2.2. La définition précédente d'un nombre algébrique se généralise à un corps quelconque. En effet, soient $\mathbb{L}$ un corps, $\mathbb{K}$ un sous-corps de $\mathbb{L}$ et $\alpha \in \mathbb{L}$. Alors α est dit algébrique sur $\mathbb{K}$ s'il est solution d'une équation polynomiale $f(x) = 0$ où f est à coefficient dans $\mathbb{K}$.
De même un entier algébrique se généralise à tout anneau.

Définition 4.2.6. *Soient B un anneau et A un sous-anneau de B, on appelle la fermeture intégrale de A dans B, l'anneau des éléments de B qui sont entiers sur A.*
Si A est intègre et si $\mathbb{K}$ est son corps de fraction, la fermeture intégrale de A dans $\mathbb{K}$ est appelée fermeture intégrale de A.
Soient B un anneau et A un sous-anneau de B, si la fermeture intégrale de A est l'anneau B tout entier, on dit qu'alors que B est entier sur A.

Définition 4.2.7. *On dit qu'un anneau A est intégralement clos s'il est intègre et si sa clôture intégrale est A lui même.*

Définition 4.2.8. *Un corps de nombre $\mathbb{K}$, ou corps de nombres algébrique, est une extension finie du corps de rationnels $\mathbb{Q}$. Autrement dit, c'est un $\mathbb{Q}-$espace vectoriel de dimension finie. La dimension de cet espace vectoriel , noté $[\mathbb{K} : \mathbb{Q}]$, est appelée degré de l'extension.*

Remarque 4.2.3. Les éléments d'un corps de nombres $\mathbb{K}$ qui sont entiers dans $\mathbb{Z}$ sont appelés entiers de $\mathbb{K}$. Ils forment un sous-anneau $\mathfrak{O}_{\mathbb{K}}$ de $\mathbb{K}$ qui est un $\mathbb{Z}$-module de rang $[\mathbb{K} : \mathbb{Q}]$.

Proposition 4.2.7. *Soient $\mathbb{K}$ un corps et $P(x) \in \mathbb{K}[X]$ un polynôme non constant. Il existe une extension algébrique $\mathbb{L}$ de $\mathbb{K}$ tels que $P(x)$ est scindé dans $\mathbb{L}[X]$.*

Définition 4.2.9. *Un corps $\mathbb{K}$ est dit algébriquement clos si tout polynôme non constant $P(x)$ à coefficients dans $\mathbb{K}$ se factorise en facteur linéaire dans $\mathbb{K}[X]$.*

Corps conjugués d'un corps de nombres

On dit que deux corps $\mathbb{L}$ et $\mathbb{M}$ contenant $\mathbb{K}$ sont conjugués sur $\mathbb{K}$ ou $\mathbb{K}$-isomorphes s'il existe un isomorphisme $\psi : \mathbb{L} \to \mathbb{M}$ tel que $\psi(x) = x$ pour tout $x \in \mathbb{K}$, en d'autre termes si ψ laisse invariant $\mathbb{K}$.

Définition 4.2.10. *Soient $\mathbb{L}$ et $\mathbb{M}$ deux extensions de $\mathbb{K}$. Deux éléments x de $\mathbb{L}$ et y de $\mathbb{M}$ sont dit conjugués s'il existe un unique $\mathbb{K}$-isomorphisme ψ tels que $\psi(x) = y$.*

Lemme 4.2.8. *Soient $\mathbb{K}$ un corps de caractéristique finie ou nulle, et $P(x) \in \mathbb{K}[X]$ un polynôme unitaire irréductible. Si $P(x)$ se décompose en facteur linéaire dans une extension $\mathbb{L}$ de $\mathbb{K}$ alors toutes ses racines sont distinctes.*

Théorème 4.2.9. *Soient $\mathbb{K}$ un corps de caractéristique finie ou nulle, $\mathbb{L}$ une extension de degré fini n de $\mathbb{K}$ et $\mathbb{M}$ un corps algébriquement clos contenant $\mathbb{K}$. Alors il existe n $\mathbb{K}$-isomorphismes distincts de $\mathbb{L}$ dans $\mathbb{M}$.*

On peut déduire de ce théorème le corollaire important suivant appelé théorème de l'élément primitif.

Corollaire 4.2.10. *Si $\mathbb{K}$ un corps de caractéristique finie ou nulle et $\mathbb{L}$ une extension de degré fini n de $\mathbb{K}$, alors il existe un élément α de $\mathbb{L}$ tels que $\mathbb{L} = \mathbb{K}(\alpha)$. α est appelé élément primitif.*

Corps quadratique

Un corps quadratique est un corps de nombre de degré 2 sur $\mathbb{Q}$, autrement engendré par une racine d'un polynôme quadratique unitaire irréductible sur $\mathbb{Q}$.

Proposition 4.2.11. *Tout corps quadratique $\mathbb{K}$ est de la forme $\mathbb{Q}(\sqrt{d})$*

La structure de l'anneau des entiers du corps $\mathbb{Q}(\sqrt{d})$ est donné par le théorème suivant :

Théorème 4.2.12. *Soit $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ un corps quadratique, avec $d \in \mathbb{Z}$ sans facteurs carrés*

(i) Si $d \equiv 2$ ou 3 (mod 4), l'anneau $\mathfrak{O}_{\mathbb{K}}$ des entiers $\mathbb{K}$ est l'ensemble des nombres de la forme $a + b\sqrt{d}$, avec $a, b \in \mathbb{Z}$.

(ii) Si $d \equiv 1$ (mod 4), $\mathfrak{O}_{\mathbb{K}}$ est l'ensemble des $\frac{1}{2}(u + v\sqrt{d})$ avec $u, v \in \mathbb{Z}$ de même parité.

Remarque 4.2.4. Un corps quadratique $\mathbb{Q}(\sqrt{d})$ est dit quadratique réel si $d > 0$ et quadratique imaginaire si $d < 0$.

Trace et Norme

Soit $\mathbb{K}$ un corps et $\mathbb{L}$ une extension de degré fini de $\mathbb{K}$ (on peut considéré le cas plus générale en travaillant avec les anneaux). Pour $\alpha \in \mathbb{L}$, on considère l'endomorphisme multiplication par α ψ_α, définit par : pour $\beta \in \mathbb{L}$, $\psi_\alpha(\beta) = \alpha\beta$.

Définition 4.2.11. *La trace et la norme d'un élément $\alpha \in \mathbb{L}$ sont définies par la trace et la norme de l'endomorphisme ψ_α respectivement.*

On peut tirer des propriétés de l'endomorphisme ψ_α certaines propriétés de la trace et la norme. En effet, soit $\alpha, \beta \in \mathbb{L}$ et $y \in \mathbb{K}$ alors

$$Tr_{\mathbb{L}/\mathbb{K}}(\alpha+\beta) = Tr_{\mathbb{L}/\mathbb{K}}(\alpha) + Tr_{\mathbb{L}/\mathbb{K}}(\beta) \quad Tr_{\mathbb{L}/\mathbb{K}}(y\alpha) = yTr_{\mathbb{L}/\mathbb{K}}(\alpha), \quad Tr_{\mathbb{L}/\mathbb{K}}(a) = n.a$$

et

$$N_{\mathbb{L}/\mathbb{K}}(\alpha\beta) = N_{\mathbb{L}/\mathbb{K}}(\alpha)N_{\mathbb{L}/\mathbb{K}}(\beta) \quad N_{\mathbb{L}/\mathbb{K}}(y\alpha) = y^n N_{\mathbb{L}/\mathbb{K}}(\alpha), \quad N_{\mathbb{L}/\mathbb{K}}(a) = a^n$$

Proposition 4.2.13. *Soient $\mathbb{L}$ une extension de degré fini n d'un corps, de caractéristique 0 ou fini, $\mathbb{K}$, $\alpha \in \mathbb{L}$ et $\alpha_1, \cdots, \alpha_n$ les racines du polynôme minimal de α sur $\mathbb{K}$ (possible dans une clôture algébrique) répétée chacune r fois, où $r = [\mathbb{K}(\alpha) : \mathbb{K}]$. Alors $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \cdots + \alpha_n$ et $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 \cdots \alpha_n$*

Proposition 4.2.14. *Soient A un anneau intègre, $\mathbb{K}$ son corps de fraction et $\mathbb{L}$ une extension de degré fini de $\mathbb{K}$. Soit $\alpha \in \mathbb{L}$ entier sur A et si de plus $\mathbb{K}$ est de caractéristique nulle, alors $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ et $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ sont entiers sur A*

Corollaire 4.2.15. *Si nous supposons de plus que A est intégralement clos alors $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ et $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ sont dans A.*

Discriminant d'un corps de nombres

Définition 4.2.12. *Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ de degré fini n et $(\alpha_1 \cdots, \alpha_n)$ dans $\mathbb{L}^n$. L'élément de $\mathbb{K}$ défini par*

$$D(\alpha_1 \cdots, \alpha_n) = det(Tr_{\mathbb{L}/\mathbb{K}}(\alpha_i\alpha_j))$$

est appelé discriminant du système $(\alpha_1 \cdots, \alpha_n)$.

Proposition 4.2.16. *Soit $(\beta_1 \cdots, \beta_n)$ un autre système de $\mathbb{L}^n$ qui vérifie $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, alors*

$$D(\beta_1 \cdots, \beta_n) = det(a_{ij})^2 D(\alpha_1 \cdots, \alpha_n)$$

Définition 4.2.13. *Soient $\mathbb{L}$ une extension d'un corps $\mathbb{K}$ de degré fini n et $(\alpha_1 \cdots, \alpha_n)$ dans $\mathbb{L}^n$. On appelle discriminant de $\mathbb{L}$ sur $\mathbb{K}$, l'idéal principal de $\mathbb{K}$ engendré par le discriminant de n'importe quelle de base de $\mathbb{L}$ sur $\mathbb{K}$, il est noté par $\mathfrak{D}_{\mathbb{L}/\mathbb{K}}$.*

Proposition 4.2.17. *Si $\mathfrak{D}_{\mathbb{L}/\mathbb{K}}$ contient un élément qui n'est pas diviseur de 0, alors il est nécessaire et suffisant, pour qu'un système $(\alpha_1 \cdots, \alpha_n) \in \mathbb{L}^n$ soit une base de $\mathbb{L}$ sur $\mathbb{K}$, que $\mathfrak{D}_{\mathbb{L}/\mathbb{K}}$ soit engendré par $D(\alpha_1 \cdots, \alpha_n)$.*

Proposition 4.2.18. *Soient $\mathbb{K}$ un corps de caractéristique nulle ou fini, $\mathbb{L}$ un extension de degré fini de $\mathbb{K}$ et $\sigma_1, \cdots, \sigma_n$ les n $\mathbb{K}$-isomorphismes distincts de $\mathbb{L}$ dans un corps algébriquement clos contenant $\mathbb{K}$. Si $(\alpha_1 \cdots, \alpha_n)$ est une base de $\mathbb{L}$ alors $D(\alpha_1 \cdots, \alpha_n) = det(\sigma_i(\alpha_j))^2$.*

Proposition 4.2.19 (Lemme de Dedekind)**.** *Considérons un groupe G, un corps K et $\sigma_1, \cdots, \sigma_n$ des morphismes distincts de G dans le groupe multiplicatif $\mathbb{K}^*$, alors les σ_i sont linéairement indépendants.*

4.2.2 Anneau de Dedekind et idéaux fractionnaires

Dans cette partie, nous présentons les anneaux de Dedekind dans le but d'obtenir un équivalent du théorème fondamentale de l'arithmétique dans ces anneaux.

Théorème 4.2.20. *Soient A un anneau et M un A-module. Alors les conditions suivantes sont équivalentes.*

1) *Toute famille non vide de sous-modules de M possède un élément maximal.*
2) *Toute suite croissante de sous-modules de M est stationnaire.*
3) *Toute sous-module de M est de type fini.*

Définition 4.2.14. *Un A-module M est noethérien si il vérifie les conditions équivalentes du théorème précédent. Un anneau A est dit noethérien s'il est un module noethérien quand il est vu comme un A-module.*

Proposition 4.2.21. *Soient A un anneau noethérien intégralement clos, $\mathbb{K}$ son corps de fraction, $\mathbb{L}$ une extension de degré fini de $\mathbb{K}$ et A' la fermeture intégrale de A dans $\mathbb{L}$. Si on suppose de plus que la caractéristique de $\mathbb{K}$ est nulle alors A' est A-module de type fini et un anneau noethérien.*

Nous rappelons qu'un idéal $\mathfrak{p}$ est premier si l'anneau quotient $A/\mathfrak{p}$ est un anneau intègre et qu'un idéal $\mathfrak{m}$ est maximal (maximal parmi les idéaux strict de A) si l'anneau quotient $A/\mathfrak{m}$ est un corps.

Lemme 4.2.22. *Considérons un anneau A, $\mathfrak{p}$ un idéal premier de A et A' un sous-anneau de A. Alors $\mathfrak{p} \cap A'$ est idéal premier de A'.*

Définition 4.2.15. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux d'un anneau A. On appelle le produit d'idéaux $\mathfrak{ab}$ l'ensemble des sommes finies $\sum(a_i b_i)$ où $a_i \in \mathfrak{a}$ et $b_i \in \mathfrak{b}$*

Remarque 4.2.5. $\mathfrak{ab}$ est un idéal de A et que $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$.
Le produit des idéaux est associatif et commutatif et possède l'anneau A tout entier comme l'élément neutre.

Soient M un A module, N un sous-module de M et $\mathfrak{a}$ un idéal de A le produit $\mathfrak{a}N$ est bien défini et c'est un sous-module de M.

Lemme 4.2.23. *Soit $\mathfrak{p}$ un idéal premier d'un anneau A et supposons que $\mathfrak{p}$ contient un produit d'idéaux $\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_\ell$. Alors $\mathfrak{p}$ contient l'un d'eux.*

Lemme 4.2.24. *Dans un anneau noethérien, tout idéal contient un produit d'idéaux premiers. Dans un anneau noethérien intègre A tout idéal non nul contient un produit d'idéaux premiers non nuls.*

Définition 4.2.16. *Soient A un anneau intègre et $\mathbb{K}$ son corps de fraction. On appelle idéal fractionnaire de A (ou par abus de langage de $\mathbb{K}$) tout sous A-module J de $\mathbb{K}$ tel qu'il existe $d \in A$ non nul qui satisfait $J \subset d^{-1}A$, en d'autre termes que tous les les élément de J ont le même dénominateur $d \in A$.*

Remarque 4.2.6. Les idéaux ordinaires de A sont les idéaux fractions avec $d = 1$ et pour un souci de confusion on les appelle souvent *idéaux entiers.*

Étant donnés deux idéaux fractionnaires I et J, leur produit est donné par l'ensemble des sommes finies $\sum(x_i y_j)$ où $x_i \in I$ et $y_i \in J$. Si les dénominateurs communs de I et J sont respectivement d et d' alors $I+J$, IJ et $I \cap J$ sont des idéaux fractionnaires de dénominateurs communs respectifs, dd', dd' et d ou d'.
Les idéaux fractionnaires non nuls de A forment monoïde commutatif pour la multiplication.

Définition 4.2.17. *Un anneau noethérien A, intégralement clos et dont tout idéal premier non nul est maximal est appelé anneau de de Dedekind.*

Théorème 4.2.25. *Soient A un anneau de Dedekind, $\mathbb{K}$ son corps des fractions, $\mathbb{L}$ une extension de degré fini de $\mathbb{K}$ et A' la fermeture intégrale de A dans $\mathbb{L}$. Supposons que $\mathbb{K}$ est de caractéristique 0, alors A' est un anneau de Dedekind et A-module de type fini.*

Remarque 4.2.7. Le théorème précédent affirme que l'anneau des entiers d'un corps de nombre est de Dedekind, mais il n'est pas toujours principal.

Théorème 4.2.26. *Dans un anneau de Dedekind A qui n'est pas un corps, tout idéal maximal de A admet un inverse dans le monoïde des idéaux fractionnaires de A*

Le point (i) du théorème suivant donne l'équivalent du théorème fondamentale de l'arithmétique aux anneaux de Dedekind.

Théorème 4.2.27. *Soient A un anneau de Dedekind et P l'ensemble des idéaux premiers non nuls de A.*

(i) Tout idéal fractionnaire non nul $\mathfrak{J}$ de A s'écrit de façon unique, à l'ordre d'apparition des idéaux prés, sous la forme

$$\mathfrak{J} = \prod_{\mathfrak{p} \in P} (\mathfrak{p}^{n_{\mathfrak{p}}(\mathfrak{J})})$$

où les $n_{\mathfrak{p}}(\mathfrak{J}) \in \mathbb{Z}$ sont tous nuls sauf un nombre fini.

(ii) Le monoïde des idéaux fractionnaires non nuls de A est un groupe.

Le théorème4.2.27 affirme que l'ensemble $fr(A)$ des idéaux fractionnaires non nuls d'un anneau de Dedekind est un groupe. Les idéaux fractionnaires principaux forment un sous-groupe $pr(A)$ distingué de ce groupe.

Définition 4.2.18. *Le groupe quotient $Cl(A) = fr(A)/_{pr(A)}$ est un groupe abélien fini appelé* ***groupe des classes d'idéaux*** *de A. L'ordre du groupe $Cl(A)$ est appelé* ***nombre des classes de*** $\mathbb{K}$ *et est noté $h_{\mathbb{K}}$*

Remarque 4.2.8.

1) Le groupe $Cl(A)$ joue un rôle important pour un anneau des entiers d'un corps de nombres car il permet de savoir, entre autres, quand est ce que cet anneau est principal. En effet, l'anneau A est principal si le groupe $Cl(A)$ est le groupe trivial, c'est à dire que si $h_{\mathbb{K}} = 1$.

2) Il existe une autre manière de définir le groupe des classes d'idéaux. On dit que deux idéaux I et J de $fr(A)$ sont équivalent s'il existe $\alpha \in A$ tels que $I = \alpha J$. Autrement dit, s'ils différent par un idéal principal. L'équivalence d'idéal fractionnaire est une relation d'équivalence et donc on peut passer au quotient.

Proposition 4.2.28. *Soient $\mathbb{K}$ un corps de nombre de degré n, et A l'anneau de ses entiers. Soit x est un élément non nul de A. Alors $N_{\mathbb{K}/\mathbb{Q}}(x) = card(A/Ax)$*

Nous savons que $N_{\mathbb{K}/\mathbb{Q}}(x) \in \mathbb{Z}$ car $x \in A$.

Définition 4.2.19. *Soit $\mathfrak{a}$ un idéal entier non nul de A. Alors, on appelle norme de $\mathfrak{a}$ le nombre $card(A/\mathfrak{a})$. On le notera par la suite par $N(\mathfrak{a})$.*

Proposition 4.2.29. *Soient $\mathfrak{a}$ et $\mathfrak{b}$ deux idéaux entiers non nuls de A, alors $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$*

4.2.3 Finitude du groupe des classes et du groupe des unités

Avant de donner les deux théorèmes principaux de la théorie, nous rappelons quelques résultats de la *géométrie des nombres*, un autre domaine de la théorie de nombres qui utilise les outils de la géométrie pour traiter des problèmes de la théorie des nombres, qui sont utilisés dans la démonstration de ces théorèmes.

Définition 4.2.20. *On appelle un réseau de $\mathbb{R}^n$, tout sous-groupe discret de rang n de $\mathbb{R}^n$.*

Théorème 4.2.30 (Minkowski)**.** *Soient L un réseau de $\mathbb{R}^n$ et S un sous-ensemble intégrable de $\mathbb{R}^n$ tels que $\mu(S) > v(L)$. Alors il existe deux éléments distincts de S tels que $x - y \in L$.*

Dans le théorème précédent, μ désigne la mesure de Lebesgue dans $\mathbb{R}^n$ et ν le "volume" du réseau L.

Corollaire 4.2.31. *Soient L un réseau de $\mathbb{R}^n$ et S une partie intégrable, symétrique par rapport à 0 et convexe de $\mathbb{R}^n$. Supposons que l'une des conditions suivantes est vérifiée :*

i) $\mu(S) > 2^n \nu(L)$

ii) $\mu(S) > 2^n \nu(L)$ *et S est compacte.*

Alors $S \cap L$ comporte un autre point autre que 0.

Soit $\mathbb{K}$ un corps de nombre de degré n, il est connu qu'il existe exactement, par le théorème de l'élément primitif, n plongements distincts $\sigma_i : \mathbb{K} \to \mathbb{C}$. Si ι désigne la conjugaison complexe alors pour tout i, il existe $j \in [1, \cdots, n]$ tel que $\sigma_i \circ \iota = \sigma_j$ et que $\sigma_j = \sigma_i$ si et seulement si $\sigma_i(\mathbb{K}) \subset \mathbb{R}$. Soit r_1 le nombre des i tels que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, alors il existe un entier r_2 tels que $n = r_1 + 2r_2$. les $2r_2$ désignent les couples du plongements complexes. Nous dirons par la suite que $\mathbb{K}$ possède r_1 plongements réels et un couple de r_2 plongements complexes et que ces $r_1 + r_2$ plongements déterminent tous les autres en posant $\sigma_{j+r_2} = \overline{\sigma_j}$ pour $r_1 + 1 \leqslant j \leqslant r_1 + r_2$. Posons

$$\sigma(x) = \big(\sigma_1(x), \cdots, \sigma_{r_1+r_2}(x)\big) \in \mathbb{R}^{r_1} \times \mathbb{C}_2^r.$$

σ est appelé plongement canonique de $\mathbb{K}$ dans $\mathbb{R}^{r_1} \times \mathbb{C}_2^r$

Proposition 4.2.32. *Soient N un sous-module libre de rang n de $\mathbb{K}$ et $(x_i)_{1 \leqslant i \leqslant n}$ une $\mathbb{Z}-$base de N. Alors $\sigma(N)$ est un réseau de $\mathbb{R}^n$ dont le volume vérifie*

$$\nu(\sigma(N)) = 2^{-r_2} \left| det_{1 \leqslant i,j \leqslant n}(\sigma_i(x_j)) \right|$$

Proposition 4.2.33. *Soient $\mathbb{K}$ un corps de nombres, de discriminant absolu d, A l'anneau des entiers de $\mathbb{K}$ et $\mathfrak{a}$ un idéal entier non nul de A. Alors $\sigma(A)$ et $\sigma(\mathfrak{a})$ sont des réseaux et vérifient*

$$\nu(\sigma(A)) = 2^{-r_2} |d|^{1/2} \qquad \nu(\sigma(\mathfrak{a})) = 2^{-r_2} |d|^{1/2} N(\mathfrak{a}).$$

Proposition 4.2.34. *Soient $\mathbb{K}$ un corps de nombres, de degré n, possédant r_1 plongements réels et un couple de r_2 plongements complexes, de discriminant absolu d et $\mathfrak{a}$ un*

idéal entier non nul de $\mathbb{K}$. *Alors* $\mathfrak{a}$ *contient un élément non nul* x *qui vérifie*

$$\left|N_{\mathbb{K}/\mathbb{Q}}(x)\right| \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}\, N(\mathfrak{a})$$

On déduit de la proposition précédente les deux corollaires suivants.

Corollaire 4.2.35. *Considérons les mêmes notations que dans la proposition précédente. Alors toute classe d'idéaux de* $\mathbb{K}$ *contient in idéal entier* $\mathfrak{J}$ *vérifiant*

$$N(\mathfrak{J}) \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |d|^{1/2}$$

Corollaire 4.2.36. *Soient* $\mathbb{K}$ *un corps de nombres, de degré* n *et* d *son discriminant absolu. Alors pour tout* $n \geqslant 2$, d *vérifie* $|d| \geqslant \dfrac{\pi}{3}\left(\dfrac{3\pi}{4}\right)^{n-1}$ *et aussi il existe une constante indépendante de* $\mathbb{K}$ *qui majore* $\dfrac{n}{\log|d|}$.

Théorème 4.2.37. *Si* $\mathbb{K}$ *est un corps de nombre de degré* $n \geqslant 2$, *alors son discriminant absolu* d *ne peut être* ± 1.

Théorème 4.2.38. *Soit* $\mathbb{K}$ *un corps de nombre. Alors le groupe des classes d'idéaux de* $\mathbb{K}$ *est un groupe abélien fini.*

Définition 4.2.21. *Les éléments inversibles de l'anneau* $\mathfrak{O}_{\mathbb{K}}$ *des entiers de* $\mathbb{K}$ *sont appelés les unités de* $\mathfrak{O}_{\mathbb{K}}$ *et souvent par abus de langage les unités de* $\mathbb{K}$ *et ces élément forment un groupe multiplicatif* $\mathfrak{O}_{\mathbb{K}}^*$.

Proposition 4.2.39. *Soient* $\mathbb{K}$ *un corps de nombres et* x *un élément de* $\mathbb{K}$. *Une condition nécessaire et suffisante pour que* x *soit une unité est qu'il soit un entier de norme* ± 1.

Le deuxième résultat majeur de la théorie algébrique de nombres est le *théorème des unités de Dirichlet*, démontré dans la première moitié du dix-neuvième, donné par l'énoncé suivant.

Théorème 4.2.40 (Dirichlet)**.** *Soient* $\mathbb{K}$ *un corps de nombres de degrés* n, *possédant* r_1 *plongements réels et un couple de* r_2 *plongements complexes et* $r = r_1 + r_2 - 1$. *Le groupe des unités* $\mathfrak{O}_{\mathbb{K}}^*$ *de* $\mathbb{K}$ *est isomorphe au produit direct* $\mathbb{Z}^r \times G$, *où* G *est un groupe cyclique fini, composé des racines de l'unité contenues dans* $\mathbb{K}$.

Les deux propositions qui suivent explicitent le groupe des unités d'un corps quadratique.

Proposition 4.2.41. *Soit $\mathbb{K} = \mathbb{Q}\sqrt{D}$ un corps quadratique imaginaire. Nous avons trois cas possibles pour le groupe G des unités de $\mathbb{K}$:*

i) Si $D \neq -1, -3$ alors $G = \{-1, 1\}$

ii) Si $D = -1$, alors $G = \{-1, 1, -i, i\}$

iii) Si $D = -3$, alors $G = \left\{-1, 1, \frac{-1-\sqrt{-3}}{2}, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}\right\}$

Proposition 4.2.42. *Soit $\mathbb{K}$ un corps quadratique réel, alors ses unités positives forment un groupe isomorphe à $\mathbb{Z}$. L'unique générateur de ce groupe est appelé unité fondamentale de $\mathbb{K}$.*

Remarque 4.2.9. Soient $\mathbb{K} = \mathbb{Q}\sqrt{D}$ un corps quadratique réel avec $D \geqslant 2$ sans facteur carré et $x = a + b\sqrt{D}$ une unité de $\mathbb{K}$. Alors $-x, x^{-1}$et $-x^{-1}$ sont aussi des unités de $\mathbb{K}$. Nous savons que $N(x) = (a + b\sqrt{D})(a - b\sqrt{D}) = \pm 1$, alors les unités mentionnés ci dessus sont de la forme $\pm a \pm b\sqrt{D}$ et qu'un seul d'entre eux est strictement supérieur à 1 pour $x \neq \pm 1$. Ainsi les unités de $\mathbb{K}$ qui sont > 1 sont de la forme $a + b\sqrt{D}$ avec a et b strictement positif.
Si $D \equiv 2, 3 \pmod 4$, comme l'anneau des entiers $\mathfrak{O}_{\mathbb{K}}$ de $\mathbb{K}$ est un $\mathbb{Z}-$module libre de base $(1, \sqrt{D})$, alors les unités $a + b\sqrt{D}$ de $\mathbb{K}$ qui sont > 1 avec $a, b > 0$ vérifient l'équation

$$a^2 - Db^2 = \pm 1$$

qui est l'équation de Pell-Fermat que nous avons étudié dans le chapitre précédent. Toutes les solutions de cet équation s'obtiennent en posant $a_n + b_n\sqrt{D} = (a_1 + b_1\sqrt{D})$ où $a_1 + b_1\sqrt{D}$ est l'unité fondamentale de $\mathbb{K}$. Si la norme de l'unité fondamentale est 1, alors l'équation $a^2 - Db^2 = -1$ n'admet des solutions.
Si $D \equiv 1 \pmod 4$, on trouve l'équation de Pell-Fermat de la forme $a^2 - Db^2 = \pm 4$ que nous avons déjà considéré dans le chapitre 3.
Ainsi toutes les solutions de l'équation de Pell-Fermat sont les unités du corps quadratique réel $\mathbb{K}$.

4.2.4 Décomposition des nombres premiers dans le corps des nombres

Soient A un anneau de Dedekind de caractéristique nulle, $\mathbb{K}$ son corps des fractions, $\mathbb{L}$ une extension de degré finie de $\mathbb{K}$ et B la fermeture intégrale de A dans $\mathbb{L}$, on a déjà vu plus haut que B est un anneau de Dedekind et que B est l'anneau des entiers de $\mathbb{L}$.
Soit $\mathfrak{p}$ un idéal premier de A, alors $B\mathfrak{p}$ est un idéal de B qui s'écrit $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{B}_i{}^{e_i}$ où les $\mathfrak{B}_i$ sont les idéaux premiers de B

Proposition 4.2.43. *Les idéaux premiers $\mathfrak{B}_i$ sont justement les idéaux $\mathfrak{J}$ de B pour lesquels $\mathfrak{J} \cap A = \mathfrak{p}$*

On peut ainsi faire correspondre à l'anneau quotient $A/\mathfrak{p}$ un sous-anneau de $B/\mathfrak{B}_i$ qui sont des corps car A et B sont de Dedekind. Ainsi On sait aussi que B est un A-module de type fini d'après le théorème 4.2.25, alors $B/\mathfrak{B}_i$ est une extension de dimension finie de $A/\mathfrak{p}$, notons f_i son degré, il est appelé degré résiduel de $\mathfrak{B}_i$ sur A. L'entier e_i qui survient dans la décomposition de $B\mathfrak{p}$ est appelé indice de ramification de $\mathfrak{B}_i$ sur A.
Il est facile de voir que $B\mathfrak{p} \cap A = \mathfrak{p}$ et que $B/B\mathfrak{p}$ est un $A/\mathfrak{p}$-espace vectoriel de dimension finie.

Proposition 4.2.44. *Avec la définition des indices ci dessus nous avons l'égalité suivante :*

$$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n$$

Proposition 4.2.45. *Avec la définition des indices ci dessus l'anneau $B/B\mathfrak{p}$ est isomorphe au produit $\prod_{i=1}^{q} B/\mathfrak{B}_i{}^{e_i}$*

Définition 4.2.22. *L'idéal premier $\mathfrak{p}$ de l'anneau A est dit ramifié dans B (ou dans $\mathbb{L}$) si l'un des indices de ramifications e_i dans $B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{B}_i{}^{e_i}$ vérifie $e_i \geqslant 2$.*

La théorie de discriminant d'un corps de nombres donne des informations sur la ramification des idéaux.

Lemme 4.2.46. *Soient A un anneau et des $B_1 \cdots B_q$ des anneaux contenants A et qui sont des A-modules libre de rang fini et $B = \prod_{i=1}^{q} B_i$ leur anneau produit alors $\mathfrak{D}_{\mathfrak{B}/\mathfrak{A}} = \prod_{i=1}^{q} \mathfrak{D}_{\mathfrak{B}_i/\mathfrak{A}}$*

Lemme 4.2.47. *Soient A et B des anneaux de sorte que B contient A et possédant une base fini $(x_1, \cdots, x_n)$, et $\mathfrak{a}$ un idéal de$A$. En posant $\bar{x}$ la classe d'un élément x de B dans $B/\mathfrak{a}B$. Alors $(\overline{x_1}, \cdots, \overline{x_n})$ est une base de $B/\mathfrak{a}B$ sur $A/\mathfrak{a}$ et on a de plus*

$$D(\overline{x_1}, \cdots, \overline{x_n}) = \overline{D(x_1, \cdots, x_n))}$$

Lemme 4.2.48. *Soient $\mathbb{K}$ un corps de caractéristique 0 ou un corps fini, et $\mathbb{L}$ une $\mathbb{K}$-algèbre de dimension finie sur $\mathbb{K}$. Alors, $\mathbb{L}$ est réduite si et seulement si $\mathfrak{D}_{\mathbb{L}/\mathbb{K}} \neq (0)$*

Définition 4.2.23. *Considérons deux corps de nombres $\mathbb{K}$ et $\mathbb{L}$ tels que $\mathbb{K} \subset \mathbb{L}$, A et B des entiers de $\mathbb{K}$ et $\mathbb{L}$ respectivement. On appelle idéal discriminant de B sur A (ou de $\mathbb{L}$ sur $\mathbb{K}$) noté par $\mathfrak{D}_{\mathfrak{B}/\mathfrak{A}}$ ou $D_{\mathbb{L}/\mathbb{K}}$ l'idéal de A engendré par les discriminant des bases de $\mathbb{L}$ sur $\mathbb{K}$ contenu dans B.*

Comme $Tr(x_i x_j) \in A$ pour toute base $(x_1, \cdots, x_n)$ de $\mathbb{L}$ sur $\mathbb{K}$ contenue dans B , alors $\mathfrak{D}_{\mathfrak{B}/\mathfrak{A}}$ est un idéal entier de A.

Théorème 4.2.49. *Conservons les mêmes notations que dans la définition précédente. Un idéal premier $\mathfrak{p}$ de A se ramifie dans B si et seulement si il contient l'idéal discriminant $\mathfrak{D}_{\mathfrak{B}/\mathfrak{A}}$. Il y a seulement un nombre fini des idéaux premiers de A qui se ramifient dans B.*

Proposition 4.2.50. *Considérons un corps de nombres $\mathbb{L}$ de degré n sur $\mathbb{Q}$ et $(x_1, \cdots, x_n)$ une base entière de $\mathbb{L}$ sur $\mathbb{Q}$. Si $D(x_1, \cdots, x_n)$ est sans facteurs carrés, alors $(x_1, \cdots, x_n)$ est une base sur $\mathbb{Z}$ de l'anneau des entiers B de $\mathbb{L}$.*

Décomposition des premiers dans un corps quadratique

Définition 4.2.24. *Soit a un entier et n un entier positif tel que $pgcd(a, n) = 1$, a est appelé résidu quadratique modulo n si l'équation $x^2 \equiv a \ (mod\ n)$ admet une solution et dans le cas où l'équation n'a pas de solutions a est appelé un non résidu quadratique.*

Le théorème suivant décrit quels nombres premiers sont ramifiés dans un corps quadratique.

Théorème 4.2.51. *Soit d un entier relatif sans facteurs carrés et posons $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ le corps quadratique engendré par $\sqrt{d}$.*

(i) Les nombres premiers impairs p pour lesquels d est un résidu quadratique modulo p et 2 si $p \equiv 1$ (mod 8) sont décomposés.

(ii) Les nombres premiers impairs p pour lesquels d est un non résidu quadratique modulo p et 2 si $p \equiv 5$ (mod 8) sont inertes.

(iii) Les diviseurs premiers impairs de d et 2 si $d \equiv 2$ ou 3 (mod 8) sont ramifiés.

Loi de réciprocité quadratique

Définition 4.2.25. *Soit p un nombre premier, pour un entier a, on définit le symbole de Legendre $\left(\frac{a}{p}\right)$ par*

$$\begin{cases} \left(\frac{a}{p}\right) = 0 & \text{si } a \text{ divise } p \\ \left(\frac{a}{p}\right) = 1 & \text{si } a \text{ est un résidu quadratique mod } p \\ \left(\frac{a}{p}\right) = -1 & \text{si } a \text{ est un non résidu quadratique mod } p \end{cases}$$

Proposition 4.2.52. *Soit $p \neq 2$ un nombre premier, alors*

1) $\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$
2) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (mod\ p)$
3) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
4) *Si $a \equiv b$ (mod p) alors* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
5) *Si $pgcd(a,b) = 1$ alors* $\left(\frac{a^2}{p}\right) = 1, \left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$
6) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$

Le théorème de réciprocité quadratique a été conjecturé par Euler et démontré par Gauss. Il permet de résoudre une large classe des équations diophantiennes quadratiques, il s'énonce comme suit :

Théorème 4.2.53 (Loi de réciprocité quadratique)**.** *Si p et q sont deux nombres premiers distincts alors*

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

Il existe une généralisation du symbole de Legendre au cas où p n'est pas un nombre premier, appelé symbole de Jacobi.

Définition 4.2.26. *Soient n et a des entiers avec n impair et positif. Par le théorème fondamentale de l'arithmétique n s'écrit $n = p_1 p_2 \cdots p_k$ où les p_i sont des nombres premiers non nécessairement distincts. Alors le symbole de Legendre est défini par*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)$$

où $\left(\frac{a}{p_i}\right)$ est le symbole de Legendre.

Corps Cyclotomique

Un exemple historique des corps de nombres est le corps cyclotomique. En effet, Gauss a introduit la cyclotomie pour la démonstration de son fameux théorème sur la construction des polygones à 17 côtés.
Considérons un corps de nombres $\mathbb{K}$. Toute racine ζ du polynôme $x^n - 1 = 0$ dans $\mathbb{K}$, pour tout entier positif n, est appelé racine de l'unité de $\mathbb{K}$. De plus, cette racine est dite primitive $n^{\text{ème}}$ de l'unité si $\zeta^p \neq 1$ pour tout $p < n$.

Remarque 4.2.10. Les racines $n^{\text{ème}}$ de l'unité d'un corps forment un groupe cyclique isomorphe à $\mathbb{Z}/n\mathbb{Z}$ dont le générateur est une racine primitive $p^{\text{ème}}$ de l'unité. L'ordre de ce groupe est $\varphi(n)$ où φ est la fonction indicatrice d'Euler.

Nous considérons dans la suite de ce paragraphe que le cas où n est un nombre premier. On peut facilement généraliser ces résultats au cas où n est composé.

Théorème 4.2.54. *Soit p un nombre premier quelconque. Alors le polynôme cyclotomique*

$$x^{p-1} + x^{p-2} + \cdots + x + 1$$

est irréductible dans $\mathbb{Q}[X]$

Définition 4.2.27. *On appelle corps cyclotomique, le corps de nombre engendré par les racines du polynôme cyclotomique, autrement les corps engendré par les racines primitives $p^{\text{ème}}$ de l'unité.*

Théorème 4.2.55. *Soient un nombre premier p et ζ une racine primitive $p^{\text{ème}}$ de l'unité. L'anneau des entiers du corps cyclotomique $\mathbb{Q}(\zeta)$ est le $\mathbb{Z}$-module libre $\mathbb{Z}[\zeta]$ dont la base est donnée par $(1, \zeta, \cdots, \zeta^{p-2})$.*

Remarque 4.2.11. Kummer avait réussi à démontrer le dernier théorème de Fermat pour une classe de nombres premiers qu'il a nommé nombre premier régulier. Un nombre premier p est dit régulier s'il ne divise pas le nombre de classe $h_{\mathbb{Q}(\zeta)}$ du corps cyclotomique $\mathbb{Q}(\zeta)$ où ζ est une racine primitive $p^{\text{ème}}$ de l'unité.

4.3 Sur les plus petits premiers qui se décomposent dans un corps quadratique imaginaire

4.3.1 Introduction

Dans son fameux traité, intitulé Disquisitiones Arithmeticae, Gauss annonça son problème de nombre des classes. Ce problème demande de lister pour tout entier positive donné n, tout les corps quadratiques imaginaires qui ont n pour nombre de classes, bien que le problème originel était énoncé dans le langage des formes quadratiques binaires. Gauss conjectura que $h(D) \longrightarrow \infty$ quand $-D \longrightarrow \infty$ et que pour certaines petites valeurs de n les listes qu'il en donna sont complète. Ce problème a une très longue histoire et des nombreux auteurs l'ont considéré.

Nous pouvons mentionner par exemple que Heilbronn [36] a résolu le problème général de manière non effective.

Le cas $n = 1$, qui est connu sous le nom du problème de nombre de classe Un de Gauss, a été résolu pour la première fois par Heegner [35], bien que sa démonstration n'a pas été accepté par la communauté de son vivant, car elle contient quelques lacunes mineures. Le problème a été résolu completement par Baker [7], en utilsant sa théorie et Stark [73].
Ils ont aussi résolu, jointement, le cas $n = 2$ [11].

Goldfeld [31] a démontré que le problème peut être réduit à l'existence d'une courbe elliptique dont la fonction L de Hasse-Weil possède un zéro d'ordre trois au point $s = 1$.

Gross et Zagier [32] ont prouvé l'existence d'une telle courbe en fonction de la dérivé

de sa fonction L de Hasse-Weil, et le problème est réduit alors a un nombre fini des calculs

Oesterlé [60] a généralisé le théorème de Goldfeld et a résolu le cas $n = 3$.

Watkins [78] a modifié l'approche de Goldfeld en considérant les fonctions L de Dirichlet avec des zéros de faible poids proche de la droite réelle pour traiter les cas $n \leq 100$.

Dans [45] Lamzouri et al ont prouvé entre autres résultats des bornes supérieurs et inférieurs pour $L(1,\chi)$ et $\zeta(1+it)$ et ont déduit des bornes explicites pour le nombre de classes des corps quadratiques imaginaires conditionnellement sur l'hypothèse Généralisé de Riemann(HGR).

Recement, Beckwith [12] a démonté une estimation pour le nombre des discriminants fondamentaux négatifs jusqu'à $-X$ dont le nombre des classes sont indivisible par un premier donné et dont le corps quadratique imaginaire satisfait un ensemble donné des conditions locales.

Dans cette section, nous démontrons une borne inférieure sur les plus petits premiers qui se décomposent dans un corps quadratique imaginaire en terme de son nombre des classes. Ce résultat est contenu dans [3].

4.3.2 Nouveau résultat

Dans cette section, nous donnons notre résultat. En effet, nous démontrons le théorème suivant.

Théorème 4.3.1. *Soit D un entier tel que $D < 0$ et $D \equiv 0,1 \pmod 4$. Soit $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ et $h_{\mathbb{K}}$ le nombre des classes de $\mathbb{K}$. Alors, les $h_{\mathbb{K}} + 1$ plus petits nombres premiers impairs qui se décomposent dans $\mathbb{K}$ vérifient l'inégalité suivante :*

$$p_{h_{\mathbb{K}}+1} \geq \frac{1}{4}\sqrt{3|D|}$$

.

Nous aurons besoin du lemme suivant dans la démonstration du théorème précédent.

Lemme 4.3.2. *Soit $G = A'X^2 + B'XY + C'Y^2$ une forme quadratique binaire primitive définie positive qui est réduite. Alors $C' \geq \frac{1}{4}\sqrt{3|D|}$*

Démonstration. Soit $D = B^2 - 4A'C'$ le discriminant de G. Alors, $-D = 4A'C' - B'^2 \geq 0 \Leftrightarrow -D \leq 4A'C'$ et par le lemme précédent nous savons que $A' \leq \sqrt{\frac{|D|}{3}}$. Ainsi, $C' \geq \frac{1}{4}\sqrt{3|D|}$ □

Démonstration. Soient D un discriminant fondamental négatif et $\mathbb{K} = \mathbb{Q}(\sqrt{D})$. Soit $h_{\mathbb{K}}$ le nombre de classes de $\mathbb{K}$. Il est bien connu qu'ils existent $h_{\mathbb{K}}$ formes réduites de discriminant D. Notons les par $F_1, ..., F_{h_{\mathbb{K}}}$.
Soit$p$ un nombre premier impair qui se décompose dans $\mathbb{K}$. Alors p peut être proprement représenté par l'une des $h_{\mathbb{K}}$ formes réduites.
Considérons $p_1, ..., p_{h_{\mathbb{K}}+1}$, les $h_{\mathbb{K}}+1$ plus petits nombres premiers qui se décomposent dans $\mathbb{K}$. Alors au moins deux nombres premiers p_i and p_j sont représentés par la même forme réduite (avec $i < j$). Soit

$$G = A'X^2 + B'XY + C'Y^2$$

la forme quadratique en question. Comme la plus petite valeur que G peut représenté est A' alors $p_i \geq A'$. Comme G représente aussi p_j, alors $p_j > A'$. Donc $p_j \geq C'$. Ainsi, par le lemme 4.3.2 nous avons$p_j \geq C' \geq \frac{1}{4}\sqrt{3|D|}$ ce qui achève la démonstration.

□

Bibliographie

[1] M. Aayad, *Sur le théorème de runge*, Acta Arithmetica **58** (1991), no. 2, 203–209.

[2] Sakha A. Alkabouss, Boualem Benseba, and Nacera Berbara, *A note on the diophantine equation* $x^2 - kxy + ky^2 + ly = 0$, (Soumis).

[3] ———, *On the small primes that split in certain imaginary quadratic fields*, (Soumis).

[4] Sakha A. Alkabouss, Tarek Garici, and Jesse Larone, *On the equation* $res_x(p(x), x^2 + sx + t) = a$, International Journal of Number Theory **14** (2018), no. 4, 1073–1079.

[5] Titu Andreescu and Dorin Andrica, *Quadratic diophantine equations*, Springer New York, 2015.

[6] Jean-Marie Arnaudiès, *Séries entiéres, séries de puiseux, séries de fourier et complémentsur les fonctions presque-périodiques*, édition marketing S.A., ellipses, 1999.

[7] Alan Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika **13** (1966), no. 2, 204–216.

[8] ———, *Linear forms in the logarithms of algebraic numbers (ii)*, Mathematika **14** (1967), no. 1, 102–107.

[9] ———, *Linear forms in the logarithms of algebraic numbers (iii)*, Mathematika **14** (1967), no. 2, 220–228.

[10] ———, *A comprehensive course in number theory*, Cambridge University Press, 2012.

[11] Alan. Baker and Harold. Stark, *On a fundamental inequality in number theory*, Annals of Mathematics **94** (1971), 190–199.

[12] O. Beckwith, *Indivisibility of class number of imaginary quadratic fields*, Research in the Mathematical Sciences **4** (2017), no. no. 20, 1–27.

[13] Manjul Bhargava, *Higher composition laws i : A new view on gauss composition, and quadratic generalizations*, Annals of Mathematics **159** (2004), no. 1, 217–250.

[14] Yuri Bilu, *Catalan's conjecture*, Séminaire bourbaki : volume 2002/2003, exposés 909-923, Unknown Month 2002, pp. 1–26 (en). talk :909.

[15] Rachid Boumahdi, Omar Kihel, and Sukrawan Mavecha, *Proof of the conjecture of keskin, Şiar and karaatli*, Annales AcademiæScientiarum FennicæMathematica **43** (2018), 1–5.

[16] Y. Bugeaud, *Approximation by algebraics numbers*, Cambridge Tracts in Matheatics 160, 2004.

[17] J. W. S. Cassels, *Introduction to diophantine approximation*, Cambridge Tracts in Matheatics and Mathematical Physics 45, 1957.

[18] H. Cohen, *Number theory : Volume i : Tools and diophantine equations*, Graduate Texts in Mathematics, Springer New York, 2007.

[19] D. Cox, *Primes of the form $x^2 + ny^2$*, John Wiley & Sons, Inc., New York, 1989.

[20] Leonard Eugene Dickson, *History of the theory of numbers, volume i : Divisibility and primality*, Chelsea Publishing Company, New York, 1952.

[21] ———, *History of the theory of numbers, volume ii : Diophantine analysis*, Dover Books on Mathematics, Chelsea Publishing Company, New York, 1971.

[22] ———, *History of the theory of numbers, volume iii : Quadratic and higher forms*, Chelsea Publishing Company, New York, 1992.

[23] N. D. Elkies, *On $a^4 + b^4 + c^4 = d^4$*, Mathematics of computation **51** (1988), no. 184, 825–835.

[24] Jan-Hendrik Evertse, *Lower bounds for resultants. II.*, Number theory. Diophantine, computational and algebraic aspects. Proceedings of the international conference, Eger, Hungary, July 29–August 2, 1996, 1998, pp. 181–198 (English).

[25] Jan-Hendrik Evertse and Kálmán György, *Lower bounds for resultants. I.*, Compositio Mathematica **88** (1993), no. 1, 1–23 (English).

[26] G. Faltings, *Endlichkeitssä für abelsche varietäten über zahlkörpern*, Inventiones Mathematicae **73** (1983), no. 3, 346–366.

[27] Masahiko Fujiwara, *Some applications of a theorem of W. M. Schmidt.*, Michigan Mathematical Journal **19** (1972), no. 4, 315–319 (English).

[28] István Gaál, *On the resolution of resultant type equations.*, Journal of Symbolic Computation **34** (2002), no. 2, 137–144 (English).

[29] István Gaál and Michael Pohst, *Solving resultant form equations over number fields.*, Mathematics of Computation **77** (2008), no. 264, 2447–2453 (English).

[30] Carl Friedrich Gauss, *Disquisitiones arithmeticæ*, Humboldt-Universität zu Berlin, 1801.

[31] D. Goldfeld, *Gauss's class number problem of imaginary quadratic fields*, Bulletin of the American Mathematical Society **13** (1985), 23–37.

[32] B. H. Gross and D. Zagier, *Heegner points and derivatives of l-series*, Inventiones Mathematicae **84** (1986), 225–320.

[33] Kálmán György, *Some applications of decomposable form equations to resultant equations.*, Colloquium Mathematicum **65** (1993), no. 2, 267–275 (English).

[34] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Fourth, Oxford, 1975.

[35] K. Heegner, *Diophantische analysis und modulfunktionen*, Mathematische Zeitschrift **56** (1952), 227–253.

[36] H. Heilbronn, *On the class number in imaginary quadratic fields*, The quartely Journal of Mathematics **5** (1934), 150–160.

[37] D. L. Hilliker and E. G. Straus, *Determination of bound for the solutions to those binary diophantine equations that satisfy the hypotheses of runge's theorem*, Transaction of American Mathematical Society **280** (1983), no. 2, 637–657.

[38] C. Houzel, *Introduction à l'hisstoire de l'analyse diophantienne*, Cahier du Séminaire d'Histoire des Mathématiques **3** (1993), 1–12.

[39] Y. Hu and M. Le, *On the diophantine equation $x^2-kxy+y^2+lx=0$*, Chinese Annals of Mathematics **34B** (2013), no. 5, 715–718.

[40] M. Jacobson and H. Williams, *Solving the pell equation*, CMS Books in Mathematics, Springer New York, 2008.

[41] O. Karaatli and Z. Şiar, *On the diophantine equation* $x^2 - kxy + ky^2 + ly = 0$, $l \in \{1, 2, 4, 8\}$, African Diaspora Journal of Mathematics **14** (2012), 24–29.

[42] K. Keskin, Z. Şiar, and O. Karaatli, *On diophantine equations* $x^2 - kxy + y^2 - 2^n = 0$, Czechoslovak Mathematical Journal **63** (2013), no. 138, 783–797.

[43] K Keskin, O Karaatli, and Z. Şiar, *On diophantine equations* $x^2 - kxy + y^2 + 2^n = 0$, Miskolc Mathematical Notes **13** (2012), no. 2, 375–388.

[44] R. Keskin, *Solutions of some quadratic diophantine equations*, Computers and Mathematics with Applications **60** (2010), no. 8, 2225–2230.

[45] Y. Lamzouri, X. Li, and K. Soundararzjan, *Conditional bounds for the least quadratic non-residue and related problems*, Mathematics of computation **84** (2015), 907–938.

[46] S. Lang and S.A. Lang, *Algebraic number theory*, Applied Mathematical Sciences, Springer, 1994.

[47] Serge Lang, *Algebra (3. ed.)*, Addison-Wesley, 1993.

[48] Hendrik W. Lenstra and Jr., *Solving the pell equation*, 2008.

[49] . LeVeque William Judson, *Fundamentals of number theory*, Addison-Wesley Reading, Mass, 1977 (English).

[50] Daniel A. Marcus, *Number fields*, Number Theory & Discrete Mathematics, Springer Verlag, New York, 1977.

[51] A. Marlewski and P. Zarycki, *Infinitely many solutions of the diophantine equation* $x^2 - kxy + y^2 + x = 0$, Computers and Mathematics with Applications **47** (2004), 115–118.

[52] S. Mavecha, *On the diophantine equation* $x^2 - kxy + ky^2 + lx = 0$, $l = 2^n$, Annals of West University of Timisoara - Mathematics and Computer Science **55** (2017), no. 1, 115–118.

[53] Pedra Mihailescu, *Primary cyclotomic units and a proof of catalan's conjecture*, Journal Reine Angewandte Mathematik **572** (2014), 167–195.

[54] Richard A. Mollin, *Quadratique diophantine equations $x^2 - d\,y^2 = c^n$*, Irish Mathematics Society Bulletin **58** (2006), 55–68.

[55] Louis Joel Mordell, *On the rational solutions of the indeterminate equations of third and fourth degrees*, Proceedings of the Cambridge Philological Society **21** (1922), 179–192.

[56] _____, *Diophantine equations*, Pure and Applied Mathematics, Elsevier Science, 1969.

[57] T. Nagel, *Introduction to number theory*, John Wiley, 1951.

[58] O. Neugebauer and A. Sachs, *Mathematical cuneiform texts*, New haven (1945).

[59] I. Niven, H.S. Zuckerman, and H.L. Montgomery, *An introduction to the theory of numbers*, Wiley, 1991.

[60] Joseph Oesterlé, *Nombres de classes des corps quadratiques imaginaires*, Séminaire bourbaki : volume 1983/84, exposés 615-632, Unknown Month 1983, pp. 309–323 (fr). talk :631. MR768967

[61] Attila Pethö, *Application of Gröbner bases to the resolution of systems of norm equations.*, ISSAC '91. Proceedings of the 1991 international symposium on Symbolic and algebraic computation. Bonn, Germany, July 15–17, 1991, 1991, pp. 144–150 (English).

[62] _____, *Systems of norm equations over cubic number fields.*, Grazer Mathematische Berichte **318** (1993), 111–120 (English).

[63] H. Poincaré, *Sur les propriétés arithmétiques des courbes algébriques*, Journal de Mathématiques Pures et Appliqués **7** (1901), 1961–233.

[64] Carl Runge, *Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen.*, Journal für die Reine und Angewandte Mathematik **100** (1887), 425–435 (German).

[65] P. Samuel, *Théorie algébrique des nombres*, Collection Méthodes, Hermann, 1971.

[66] Andrzej Schinzel, *An improvement of runge's theorem on diophantine equations*, Pontificia Accademia delle Scienze, Pontificia Acad. Scientiarum, 1968.

[67] Hans P. Schlickewei, *Inequalities for decomposable forms.*, Astérisque **41-42** (1977), 267–271 (English).

[68] Wolfgang M. Schmidt, *Inequalities for resultants and for decomposable forms.*, in Proc. Conf. Diophantine Approx. Appl., Proc. Conf. Washington 1972, 235-253 (1973)., 1973, pp. 233–253 (English).

[69] T. N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Tracts in Mathematics, Cambridge University Press, 1986.

[70] C. L. Siegel, *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, Journal of London Mathematical Society **1** (1926), 66–68.

[71] ———, *über einige anwendungen diophantischer approximationen*, Abh. Pr. Akad. Wiss **1** (1929), 41–69.

[72] Vladmir G. Sprindžuk, *Classical diophantine equation*, Springer-Verlag Berlin Heidelberg New York, 1993.

[73] Harold. Stark, *On the class number in imaginary quadratic fields*, Michigan Mathematical Journal **14** (1967), 1–27.

[74] Sz. Tengely, *On the diophantine equation* $f(x) = g(x)$, Acta Arithmetica **110** (2003), no. 2, 185–200.

[75] Axel Thue, *über annäherungswerte algebraischer zahlen.*, Journal für die reine und angewandte Mathematik **135** (1909), 284–305 (ger).

[76] R. Tidjdeman, *On the equation of catalan*, Acta Arithmetica **29** (1976), no. 2, 197–209.

[77] P. G. Walsh, *A quantitative vesion of runge's theorem on diophantine equations*, Acta Arithmetica **62** (1992), no. 2, 157–172.

[78] M. Watkins, *Class number of imaginary quadratic fields*, Mathematics of computation **73** (2003), 907–938.

[79] André Weill, *Number theory : an approach trough history from hammurapi to legendre*, Boston, BIRKHÄUSER, 1983.

[80] A. Wiles, *Modular elliptic curve and fermat's last theorem*, Annals of Mathematics **141(3)** (1995), no. 2, 443–551.

[81] A. Wiles and R Taylor, *Modular elliptic curve and fermat's last theorem*, Annals of Mathematics **141(3)** (1995), no. 2, 553–572.

[82] Eduard A. Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree.*, in 1969 Number Theory Institute, Proceedings of Symposia in Pure Mathematics : Vol. : 20 :, 1971, pp. 213–247 (English).

[83] P. Yuan and Y. Hu, *On the diophantine equation* $x^2 - kxy + y^2 + lx = 0$, $l \in \{1, 2, 4\}$, Computers and Mathematics with Applications **61** (2011), 573–577.

UNIVERSITE CHEIKH ANTA DIOP DE DAKAR
FACULTÉ DES SCIENCES ET TECHNIQUES
ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE
THÈSE DE DOCTORAT UNIQUE
Spécialité: Codage, Cryptologie, Algèbre et Applications

Nom et prénoms du Candidat: Aboussaghid Alkabouss Sakha
Titre de la thèse: Équations Diophantiennes: Formes quadratiques et Nombres de classes
Date et Lieu de soutenance: Le 11 mars 2019 à l'amphi 7.

JURY

PRÉSIDENT	Pr. Mamadou SANGHARÉ	Université Cheikh Anta Diop, Sénégal
RAPPORTEURS	Pr. Farid BENCHERIF	Université de Sciences et Technologie Houari Boumediene, USTHB, Algérie
	Pr. Kacem BELGHABA	Université Oran I, Algérie
EXAMINATEURS	Pr. Oumar DIANKHA	Université Cheikh Anta Diop, Sénégal
	Pr. Ismaïla DIOUF	Université Cheikh Anta Diop, Sénégal
	Dr. Abdoul Aziz CISS	Ecole polytechnique de Thiès, Sénégal
DIRECTEURS DE THÈSE	Pr. Omar KIHEL	Brock University, Canada
	Pr. Djiby SOW	Université Cheikh Anta Diop, Sénégal

Résumé:

L'analyse diophantienne est la branche de la théorie des nombres qui traite, en particulier, les équations polynomiales à coefficients entiers et dont les solutions recherchées sont entières. Ce genres d'équations sont appelées équations diophantiennes. Le manque d'une méthode générale pour résoudre une équation diophantienne quelconque ouvre la voie à la mise en place des méthodes spécifiques. Pour certaines familles d'équations diophantiennes ces méthodes spécifiques existent.

Dans cette thèse, nous avons apporté les contributions suivantes.

Soient $Res_x(P(x), Q(x))$ le résultant en x de deux polynômes, s, t et a des entiers rationnels. En utilisant une amélioration de la méthode de Runge due à Schinzel, nous avons démontré que l'équation diophantienne de type résultant, donnée par $Res_x(P(x), x^2+sx+t) = a$ admet un nombre fini de solutions entières.

Nous avons étudié aussi l'équation diophantienne $x^2-kxy+ky^2+ly = 0$ où k et l sont des entiers avec k pair. Nous avons également considéré la même équation quand $l = 3^n$ et $k \equiv 2$ (modulo 3); $l = 2^r3^s$ et $k = 2k' + 1$ avec $k' \equiv 2$ (modulo 3) où n, r et s sont des entiers positifs. Nous avons utilisé la théorie des équations de Pell-Fermat généralisées pour fournir une caractérisation des solutions entières de ces équations.

Enfin, nous avons obtenu une borne inférieure sur les $h + 1$ plus petits nombres premiers qui se décomposent dans un corps quadratique imaginaire où h désigne le nombre des classes de ce corps.

Abstract:

Diophantine analysis is the branch of number theory which deals with, in particular, polynomial equations with integer coefficients and for which the solutions are also integers. Such equations are called Diophantine equations. The lack of general method to solve any Diophantine equation open the way to come up with specific methods. For the some family of Diophantine equations such methods exist.

In the thesis, we brought the following contributions.

Let $Res_x(P(x), Q(x))$ be the resultant of two polynomials in x, s, t and a be rational integers. Using an improvement of Runge's theorem due to Schinzel, we have proved that the resultant Diophantine equation, given by $Res_x(P(x), x^2 + sx + t) = a$, has only a finite number of integer solutions.

We have, also, studied the Diophantine equation $x^2 - kxy + ky^2 + ly = 0$, where k and l are integers with k even. We considered the same equation when $l = 3^n$ and $k \equiv 2$ (modulo 3); $l = 2^r3^s$ et $k = 2k'+1$ with $k' \equiv 2$ (modulo 3) where n, r and s are positive integers. We used the theory of generalized Pell-Fermat equations to obtain a characterisation of integer solutions of these equations.

Finally, We get a lower bound on the first $h+1$ prime numbers that split in some imaginary quadratic fields, where h denotes the class number of this fields.