N° d'ordre : /2017-D/MT

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumedienne

Faculté des Mathématiques

Thèse présentée pour l'obtention de grade de Docteur en Mathématiques

Spécialité : Algèbre et Théorie des Nombres

Par

HAMTAT Abdelkader

THÈME

SUR LES EQUATIONS DIOPHANTIENNES

Soutenu publiquement, le..... devant le jury composé de :

Mr.	Kamel BETINA	Professeur	U.S.T.H.B.	Président.
Mr.	Djilali BEHLOUL	Professeur	U.S.T.H.B.	Directeur de thèse.
Mr.	Abbes BENAISSA	Professeur	U.Sidi Bel Abbes	Examinateur.
Mr.	Seddik OUAKKAS	Professeur	U.Saida	Examinateur.
Mr.	Noureddine AMROUN	MCA	U.Sidi Bel Abbes	Examinateur.
Mr.	Med Salem REZAOUI	MCA	U.S.T.H.B.	Examinateur.

Remerciements

Je tiens

Table des matières

Introduction

Les équations Diophantiennes trouvent leur origine dans l'Antiquité, elles portent leur nom en l'honneur de mathématicien grècque Diophante.

Une équation Diophantienne est une équation que l'on peut former à partir d'inconnus, de nombres entiers, et des deux opérations $+$ et $\times$. Plus formellement, étant donné un polynôme $P \in \mathbb{Z}[X_1, ..., X_n]$, on demande de trouver tous les $n-uplets$ $(x_1, ..., x_n)$ dans $\mathbb{Z}^n$ tels que

$$P(x_1, ..., x_n) = 0.$$

Au cours des siècles, la résolution des équations Diophantiennes a occupé beaucoup de mathématiciens. La plus fameuse équation Diophantienne et sans doute l'équation de Fermat

$$x^n + y^n = z^n, \qquad n \geq 3.$$

Au XVII siècle, Pierre de Fermat a cojucturé que cette équation n'a pas de solutions non triviales. Cette équation et bien d'autres ont été durant plus de trois siècles des moteurs du développement de la théorie des nombres moderne, si l'on énumère tous les outils introduits et utilisés en vu de la résolution de cette conjecture, on trouve la majorité de la théorie algébrique des nombres, des courbes elliptiques, des formes modulaires, de la géométrie algébrique... et beaucoup d'autres notions.

Le problème fondamental dans les équations Diophantiennes est qu'une telle équation est-elle résoluble ou non ? et si elle est résoluble, l'ensemble des ses solutions est-il fini ou non ? et le déterminer.

L'équation Diophantienne $f(x) = y^n$. Soit f un polynôme irréductible à coefficients dans $\mathbb{Z}$, de degré $m \geq 2$. Soit $n \geq 2$ un entier, les travaux de Siegel [12] affirment que l'équation

$$f(x) = y^n, \quad x, y \in \mathbb{N},$$

a un ensemble fini de solutions, dans le cas où $(m, n) \neq (2, 2)$, en particulier, les équation de la forme

$$ax^2 + bx + c = dy^n, \ n \geq 3, \tag{0.0.1}$$

où a, b et c sont des entiers naturels tels que $a \neq 0$, $b^2 - 4ac \neq 0$ et $d \neq 0$, a un ensemble fini de solutions si $n \geq 3$. Il est bien connu qu'il n'y a pas en général une méthode pour déterminer toutes les solutions de (0.0.1), mais plusieurs cas particuliers d'une telle équation ont été etudiées depuis longtemps.

Dans cette thése, nous résolvons complètement l'équation Diophantienne

$$x^2 + 13^k = y^n, \quad n \geq 3. \tag{0.0.2}$$

Une équation de la forme

$$x^2 + C = y^n, \ n \geq 3 \tag{0.0.3}$$

avec $C = 13^k$, et nous donnons toutes les solutions possibles pour tout entier k.

C'est un cas particulier de l'équation (0.0.3) qui a une longue histoire, le premier cas qui a été résolu apparu en 1850 est pour $C = 1$, *V. Lebesque [25]* montre que l'équation $x^2 + 1 = y^n$, $n \geq 3$ a une seule solution $(x, y) = (1, 0)$ en utilisant les méthodes élémentaires de la théorie algèbrique, en particulier, la propriété de l'unicité de la factorisation dans les anneaux de Dedekind. En 1993, *J-H-Cohn* [13], [16] a résolu cette équation pour 77 valeurs de C comprises entre 0 et 100. D'autres travaux ont été faits pour certaines valeurs restantes de C comme par exemple *(Siksek-Cremona)[34]* pour $C = 7$, *(Mignotte- De Weger)[31]* pour $C = 74, 85$, *(Bennett, Skinner)[6]* pour $C = 55, 95$.

Depuis peu, certains auteurs ont considéré l'équation (0.0.3) pour des valeurs de C, où C est une puissance d'un nombre premier q. *J-H- Cohn* [14] a prouvé que si $C = 2^{2k+1}$, alors l'équation (0.0.3) a une solution sauf si $n = 3$, dans ce cas il y a trois familles de solutions, et Abu Muriefah [2] a conjucturé que les seules solutions pour $C = 2^{2k}$ sont données par $(x, y) = (2^k, 2^{2k+1})$ et $(x, y) = (11.2^{k-1}, 5.2^{2(k-1)/3})$ et cela pour $(k, n) = (3M+1, 3)$. En [27],

Luca pouvait démontrer la conjecture de *Abu Muriefa* concernant l'équation $x^2 + 3^{2m} = y^n$, entre temps, Luca a résoulu complétement l'équation (0.0.3) pour $C = 2^a.3^b$ sous la condition que x et y soient premier entre eux. Pour $C = 3^{2k+1}$, *Abu Muriefah et Arif* [4] ont démontré que l'équation (0.0.3) a exactement une famille de solutions, le cas où $C = 3^{2k+1}$ avec x, y premiers entre eux, a été résolu par *Luca* [29]. Beaucoup d'autres résultats ont été etablis par plusieurs auteurs.

Les deuxiémes équations que nous avons résolu sont des équations en nombres triangulaires de la forme

$$T_X + T_Y = T_Z, \qquad T_X = \frac{X(X+1)}{2}, \quad X \in \mathbb{N}, \tag{0.0.4}$$

Les méthodes de résolution sont totalement différentes de celles des premières équations, sont des méthodes purement combinatoires. L'idée de cette équation vient de la fameuse équation de Pythagore $X^2 + Y^2 = Z^2$, si on change le carré par le triangle on obtient l'équation (0.0.4). Nous arriverons à prouvé que cette équation a une infinité de solutions entières , et nous construisons des nouvelles suites.

Organisation de la Thèse. La thèse est composée de trois chapitres, le premier chapitre est consacré à la méthode de résolution de l'équation (0.0.3) introduite par Cohn, et certains rappels sur la théorie algébrique des nombres, ainsi qu'une méthode de calcul du nombre de classes d'idéaux d'un corps quadratique imaginaire.

Le second chapitre traite l'équation $x^2 + 13^k = y^n$, $n \geq 3$. [18] Celui-ci contient une résolution detaillée et complète de l'équation $x^2 + 13^k = y^n$, $n \geq 3$ en utilisant la méthode de la factorisation dans les anneaux de Dedekind et le théorème du diviseur primitif. En particulier nous démontrons les deux theorèmes suivants

Théorème 0.0.1 *Soit m un entier positifs, l'équation Diophantienne*

$$x^2 + 13^{2m} = y^n, \tag{0.0.5}$$

où $n \geq 3$, n'a pas de solution en entiers positifs .

Théorème 0.0.2 *Soit m un entier positifs, l'équation diophantienne*

$$x^2 + 13^{2m+1} = y^n, \tag{0.0.6}$$

où $n \geq 3$ a excactement une famille de solutions donneé par

$$(x, y, m, n) = (70 \cdot 13^{3k}, 17 \cdot 13^{2k}, 3k, 3).$$

Le troisième chapitre quant à lui contient quelques propriétés et identités concernant les nombres triangulaires. Puis, nous donnerons plusieurs résolutions de l'équation Diophantienne (0.0.4) [19] en utilisant la méthode de résolution paramétrique et une méthode spéciale et originale permettant de construire des familles infinies de solutions. Des nouvelles suites d'entiers sont déterminées, cette résolution nous permet de donner le résultas suivant

Théorème 0.0.3 *Il existe certaine matrice carée M d'ordre 3, à éléments dans $\{1, 2, 3\}$, telle que si* $\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ *est une solution de (0.0.4) alors M* $\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ *est aussi une solution.*

En déterminant la matrice M, nous pouvons déterminer des familles infinies de solutions de l'équation (0.0.4).

On terminera par une conclusion et des perspectives.

Chapitre 1

Sur l'équation Diopahntienne

$$x^2 + C = y^n, n \geq 3$$

1.1 Introduction

Dans ce chapitre, nous allons donner un rappel sur les outils essentiels utilisés dans la résolution de l'équation $x^2 + C = y^n, n \geq 3$ étudié par *J.H.Cohn* [13], [16] en 1993. Nous commençons par donner quelques notions élémentaires de la théorie algébrique des nombres tels que les idéaux fractionnaires et les groupes de classes d'idéaux. Pour calculer le nombre de classes du corps quadratique imaginaire $\mathbb{Q}(\sqrt{-C})$ noté $h(\mathbb{Q}(\sqrt{-C}))$ qu'on aura besoin pour vérifier qu'un anneau est principal donc factoriel, nous rappelerons la notion des formes quadratiques binaires, et le résultat principal qui affirme que $h(\mathbb{Q}(\sqrt{-C}))$ est égal au nombre de classes de formes quadratiques binaires définies positives de discriminant du corps $\mathbb{Q}(\sqrt{-C})$.

Ensuite, nous allons rappeler les résultats de Cohn concernant l'équation (0.0.3), ainsi que quelques exemples qui n'ont pas été résolus par lui pour des différentes valeurs de C.

1.2 Rappels

Définition 1.2.1 *Soit $T(X)$ un polynôme irréductible de degré n à coefficients rationnels, et soit θ une racine complexe de T. On note $K = \mathbb{Q}(\theta)$ l'ensemble des fractions rationelles en θ à coefficients dans $\mathbb{Q}$.*

Si $\theta = \theta_1, ..., \theta_n$ sont les racines complexes de T, l'application σ_i telle que $\sigma_i(A(\theta)) = A(\theta_i)$ est un plongement complexe de K dans $\mathbb{C}$. De plus, si $\theta_i \in K$, pour tout i, on dit que K est une extension galoisienne de $\mathbb{Q}$, dans ce cas σ_i sont des automorphismes de K qui forment le groupe de Galois $K/\mathbb{Q}$ de K.

Définition 1.2.2 *Soit $\alpha \in K = \mathbb{Q}(\theta)$. On appelle norme de α et on note $N_{K/\mathbb{Q}}(\alpha)$ le déterminant de l'application $\mathbb{Q}-$linéaire : $x \longmapsto \alpha x$ de K dans K.*

D'aprés la définition, on voit que la norme est multiplicative i-e $N_{K/\mathbb{Q}}(\alpha\beta) = N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta)$ et que $N_{K/\mathbb{Q}}(\alpha) = \prod_{1\leq i\leq n} \sigma_i(\alpha)$.

Définition 1.2.3 *On dit que $\alpha \in K$ est un entier algébrique s'il est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$. On note par $\mathbb{Z}_K$ l'anneau des entiers algébriques de K.*

Définition 1.2.4 *(1) On dit qu'un sous- ensemble $\mathfrak{a}$ est un idéal de $\mathbb{Z}_K$ si c'est un sous groupe additif stable par la multiplication externe par $\mathbb{Z}_K$.*

(2) On dit que $\mathfrak{a}$ est un idéal principal s'il est de la forme $\mathfrak{a} = \alpha\mathbb{Z}_K$, pour $\alpha \in \mathbb{Z}_K$.

Si $\mathfrak{a}$ et $\mathfrak{b}$ sont deux idéaux, on appellera produit de $\mathfrak{a}$ et $\mathfrak{b}$, et le on notera $\mathfrak{ab}$, l'ensemble des combinaisons linéaires finies $\sum_i a_i b_i$ avec $a_i \in \mathfrak{a}$ et $b_i \in \mathfrak{b}$.

Proposition 1.2.1 *Si $\mathfrak{a}$ est un idéal (non nul) l'anneau quotient $\mathbb{Z}_K/\mathfrak{a}$ est fini. En particulier, $\mathfrak{p}$ est un idéal premier non nul si et seulement si $\mathbb{Z}_K/\mathfrak{p}$ est un corps fini.*

Ceci nous conduit à la définition suivante

Définition 1.2.5 *Si $\mathfrak{a}$ est un idéal non nul de $\mathbb{Z}_K$ on appelle norme de $\mathfrak{a}$, et on note $N(\mathfrak{a})$, le nombre d'éléments de l'anneau quotient $\mathbb{Z}_K/\mathfrak{a}$.*

Proposition 1.2.2 *(1) La norme est multiplicative sur les idéaux :* $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.

(2) Si $\mathfrak{a} = \alpha\mathbb{Z}_K$ *est un idéal principal on a* $N(\mathfrak{a}) = |\mathcal{N}(\alpha)|$.

(3) Si $\mathfrak{p}$ *est un idéal premier, on a* $N(\mathfrak{p}) = p^f$ *, où* p *est la caractéristique du corps fini* $\mathbb{Z}_K/\mathfrak{p}$, *et* $f = \dim(\mathbb{Z}_K/\mathfrak{p})$.

Le travail dans un corps de nombres nous amène à généraliser la définition d'un idéal. Si $\mathfrak{a}$ un idéal et $m \in \mathbb{Z}_{>0}$, on définit l'idéal $\mathfrak{a}/m$ appelé idéal fractionnaire, pour ne pas confondre les idéaux entiers (ordinnaires) définis ci-dessus, ainsi, toutes les propriétés se généralisent de façon naturelle aux idéaux fractionnaires.

Nous avons introduit cette notion pour donner le théorème suivant, qui regroupe les propriétés essentielles des idéaux fractionnaires.

Théorème 1.2.1 *(1) Les idéaux fractionnaires non nuls de* K *forment un groupe abélien* $I(K)$ *pour la multiplication des idéaux.*

(2) Toute idéal (non nul) $\mathfrak{a}$ *de* K *s'écrit d'une manière unique sous la forme* $\mathfrak{a} = \prod_{\mathfrak{p}} p^{v_{\mathfrak{p}}(\mathfrak{a})}$, *où les idéaux* p *sont les idéaux premiers distincts de* $\mathbb{Z}_K$ *et* $v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$.

(3) Si on note $\Pr(K)$ *le sous groupe de* I *formé des idéaux principaux, le groupe quotient* $Cl(K) = I(K)/\Pr(K)$ *est un sous groupe abélien fini, appelé groupe de classes d'idéaux de* K.

Ce théorème nous montre que l'existence et l'unicité de la décomposition en facteurs premiers n'est pas vraie en général dans $\mathbb{Z}_K$. D'autre part, le groupe de classes $Cl(K)$ nous donne un outil de savoir qu'un anneau d'entiers est principal. Notons le résultat suivant :

Proposition 1.2.3 *Le groupe de classes d'idéaux* C_K *est fini.*

Proposition 1.2.4 *Soit* $h(K) = |Cl(K)|$ *le nombre de classe de* K.

(1) Si $h(K) = 1$ *alors* $\mathbb{Z}_K$ *est un anneau principal,*

(2) Pour tout idéal $\mathfrak{a}$ *de* K *l'idéal* $\mathfrak{a}^{h(K)}$ *est un idéal principal.*

(3) Si m *un entier premier avec* $h(K)$, *alors pour tout idéal* $\mathfrak{a}$ *de* K, *l'idéal* $\mathfrak{a}^m$ *est un idéal principal.*

(4) Soit K *un corps de nombres et* $\mathfrak{a}_1, \mathfrak{a}_2$ *des idéaux fractionnaire non nuls. Supposons qu'il existe un idéal fractionnaire non nul* $\mathfrak{b}$ *et un entier* m *tels que* $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{b}^m$. *Alors il existe deux idéaux fractionnaires* $\mathfrak{b}_1$ *et* $\mathfrak{b}_2$ *tels que* $\mathfrak{a}_1 = \mathfrak{b}_1^m$ *et* $\mathfrak{a}_2 = \mathfrak{b}$.

Un autre groupe essentiel dans la théorie algébrique des nombres et même pour la résolution des équations Diophantiennes est le groupe des unités d'un corps de nombres.

Définition 1.2.6 *On dit que $u \in \mathbb{Z}_K$ est une unité si u est inversible dans $\mathbb{Z}_K$. L'ensemble des unités de $\mathbb{Z}_K$ forment un groupe noté $U(K)$.*

Il est facile de voir qu'un élément u de $\mathbb{Z}_K$ est une unité si et seulement si $N(u) = \pm 1$. L'importance du groupe des unités réside dans le fait évident que deux éléments α et β engendrent le même idéal principal si et seulement si α/β est une unité.

La factorisation de l'équation $x^2 + C = y^n$ en cours de la résolution, nous conduit à travailler dans le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-C})$ où $C > 0$ sans facteurs carrés, ainsi pour le calcul de nombre de classes d'idéaux d'un tel corps nous avons besoin des résultats suivants :

Soit K une extension quadratique de $\mathbb{Q}$, c'est- à-dire une extension de degré 2 de $\mathbb{Q}$. Nous allons étudier l'ensemble des entiers de K.

Proposition 1.2.5 *Soit K une extension quadratique de $\mathbb{Q}$. Il existe $d \in \mathbb{Z}\setminus\{0,1\}$ et d sans facteurs carrés tel que $K = \mathbb{Q}(\sqrt{d})$ (où d désigne un complexe dont le carré est d).*

Définition 1.2.7 *(Corps quadratiques réels, complexes). On dit que $\mathbb{Q}(\sqrt{d})$ est un corps quadratique réel (resp. complexe) si $d > 0$ (resp. $d < 0$).*

Proposition 1.2.6 *Soit $d \in \mathbb{Z}\setminus\{0,1\}$ sans facteurs carrés. Une $\mathbb{Z}$-base d'entiers de $\mathbb{Q}(\sqrt{d})$ est donnée par $(1, \sqrt{d})$ si $d \equiv 2, 3 (\mathrm{mod}\, 4)$, et par $\left(1, \dfrac{1+\sqrt{d}}{2}\right)$ si $d \equiv 1 (\mathrm{mod}\, 4)$. Les discriminants de ces corps sont $4d$ si $d \equiv 2, 3 (\mathrm{mod}\, 4)$ et d si $d \equiv 1 (\mathrm{mod}\, 4)$.*

Proposition 1.2.7 *Soit $d < 0$ un entier sans facteurs carrés et $K = \mathbb{Q}(\sqrt{d})$. Alors $U(K) = \{-1, +1\}$ sauf dans les deux cas suivants :*

(i) $d = -1$, donc $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-1}]$, et alors $U(K) = \{-1, 1, i, -i\}$;

(ii) $d = -3$, donc $\mathbb{Z}_K = \mathbb{Z}\left[\dfrac{1+\sqrt{-3}}{2}\right]$, et alors $U(K) = \{\pm 1, \pm\omega, \pm\omega^2\}$ où $\omega = e^{\frac{i\pi}{3}}$.

Formes quadratiques binaires à coefficients entiers

Définition 1.2.8 *Une forme quadratique binaire à coefficients entiers est une fonction de la forme*

$$\varphi(x,y) = ax^2 + bxy + cy^2, \quad (a,b,c) \in \mathbb{Z}.$$

On note la forme φ par (a,b,c). Le discriminant de la forme (a,b,c) est $D = b^2 - 4ac$, elle est définie positive si $D < 0$ et $a > 0$. Dans ce cas, on a aussi $c > 0$ et $\varphi(x,y) > 0$ si $(x,y) \neq (0,0)$.

On dit que l'entier n est représentable par la forme (a,b,c) s'il existe $(x,y) \in \mathbb{Z}$ tel que $n = ax^2 + bxy + c$.

Soit $f : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^2$ une application. Elle est dite unimodulaire si son déterminant vaut 1. En notant $f(x,y) = (px + qy, rx + sy)$, cela se traduit par $ps - qr = 1$. En particulier, f est inversible.

Les exemples les plus simples de transformations unimodulaires sont

$f_1 = (x,y)$, $f_2(x,y) = (x+y,y)$ et $f_3(x,y) = (x-y,y)$.

Si dans $\varphi(x,y) = qx^2 + bxy + cy^2$, on remplace x par $px^{'} + qy$ et y par $rx^{'} + sy^{'}$, on obtient une nouvelle forme quadratique $\varphi^{'}(x^{'},y^{'}) = a^{'}x^{'2} + b^{'}x^{'}y^{'} + c^{'}y^{'2}$ avec

$$\begin{aligned} a^{'} &= ap^2 + bqr + cr^2 = \varphi(p,r) \\ b^{'} &= 2apq + b(ps + qr) + 2crs \\ c^{'} &= aq^2 + bqs + cs^2 = \varphi(q,s). \end{aligned}$$

Définition 1.2.9 *Deux formes quadratiques φ et $\varphi^{'}$ sont dites équivalentes s'il existe une transformation unimodulaire f telle que $\varphi \circ f = \varphi^{'}$. On notera $\varphi \sim \varphi^{'}$.*

Par example en utilisant f_1, f_2 et f_3, on a les transformations suivantes.

$(T1)$ $(a,b,c) \sim (c,-b,a)$,

$(T2)$ $(a,b,c) \sim (a,b+2a,a+b,c)$,

$(T3)$ $(a,b,c) \sim (a,b-2a,a-b,c)$.

Lemme 1.2.1 *La relation $\sim$ est une relation d'équivalence qui conserve le discriminant.*

Proposition 1.2.8 *Toute forme quadratique définie positive est équivalente à une forme* (a, b, c) *vérifiant*

$$-a < b \leq a < c \quad ou \quad 0 \leq b \leq a = c.$$

Lemme 1.2.2 *Deux formes quadratiques définies positives réduites sont non équivalentes.*

Proposition 1.2.9 *Il n'existe qu'un nombre fini de classes d'équivalences de formes quadratiques de discriminants* $D < 0$ *donné. Ce nombre, not e* h_D *est égal au nombre de solutions* $(a, b, c) \in \mathbb{N}^* \times \mathbb{Z} \times \mathbb{N}^*$ *du système d'équation*

$$\begin{cases} b^2 - 4ac = D \\ a \leq \sqrt{-D/3}. \\ -a < b \leq a < c \text{ ou } 0 \leq b \leq a = c. \end{cases}$$

Preuve. Toute forme est équivalente à une forme réduite et les formes réduites sont non équivalentes entre elles, le nombre de classes d'équivalences de forme de discriminant D est donc le nombre de formes réduites $\varphi = (a, b, c)$ de discriminant D.

On a alors $b^2 - 4ac = D$. Par les formules du théorème 1.3.2,

$$|b| \leq a \text{ et } |b| \leq c \Longrightarrow b^2 \leq ac,$$

d'où $-3ac \geq D$ puis $ac \leq -D/3$. Mais $0 \leq a \leq c$, donc $a \leq \sqrt{-D/3}$ et a ne peut prendre qu'un nombre fini de valeurs; il en est de même de b puisque $|b| \leq a$, et de c puisque $b^2 - 4ac = D$. ■

Proposition 1.2.10 *Soit* $K = \mathbb{Q}(\sqrt{d})$ *où* $d < 0$ *sans facteurs carrés, un corps quadratique imaginaire. Alors le nombre de classes de* $Cl(K)$ *est égal au nombre de classes de formes quadratiques.*

Proposition 1.2.11 *Soit* $K = \mathbb{Q}\left(\sqrt{d}\right)$ *avec* $-2006 \leq d \leq -1$ *et* d *sans facteurs carrés. Alors* $\mathbb{Z}_K$ *est principal si et seulement si* $d = -163, -67, -43, -19, -11, -7, -3, -2$ *ou* -1.

1.3 Méthodes et difficultés

Cohn [13], [16] a étudie l'équation (0.0.3) où x, y sont premiers entre eux et $1 \leq C \leq 100$, il a résolu l'équation (0.0.3) pour 77 valeurs de C. Ses méthodes sont inventives et élémentaires, mais elles ne lui ont pas permis de résoudre l'équation (0.0.3) pour certaines valeurs de C. (Nous donnons par la suite quelques résultas concernant les valeurs de C dont les méthodes de Cohn ne peuvent pas s'appliquer).

L'idée principal de la résolution de l'équation (0.0.3) repose sur la factorisation dans le corps quadratique imaginaires $\mathbb{Q}(\sqrt{-C})$, alors l'equation (0.0.3) devient

$$(x + \sqrt{-C})(x - \sqrt{-C}) = y^p$$

Comme on a la notion de la principalité des idéaux, on peut conclure qu'il existe des entiers naturels a et b vérifient

$$\pm x + \sqrt{-C} = (a + b\sqrt{-C})^p, \tag{1.3.1}$$

alors x est une solution avec $y = a^2 + b^2C$. Mais cette condition n'est pas nécessaire pour que l'équation (1.3.1) admette une solution, c'est le cas sauf si :

i) $C \not\equiv 3 (\mathrm{mod}\, 4)$,

ii) *Le problème des unités ne se pose pas,*

iii) *Le corps quadratique* $\mathbb{Q}(\sqrt{-C})$ *a une unique factorisation,*

iv) *les facteurs* $x \pm \sqrt{-C}$ *n'ont pas un facteur commun,*

v) C *n'est pas un carré parfait.*

Mais ce qui est vrai dans tous les cas, c'est que (1.3.1) est une condition suffisante pour une solution.

Supposons que $C \equiv 3 (\mathrm{mod}\, 4)$, alors l'anneau des entiers quadratique est donné par $\mathbb{Z}[\sqrt{-C}] = \{\frac{1}{2}(a + b\sqrt{-C}), a \equiv b \equiv 1 (\mathrm{mod}\, 2)\}$, donc on obtient en ajoutant à (1.3.1) une nouvelle condition suffisante suivante

$$\pm x + \sqrt{-C} = (\frac{1}{2}(A + B\sqrt{-C}))^p, \quad A \equiv B \equiv 1 (\mathrm{mod}\, 2), \tag{1.3.2}$$

avec

$$\begin{aligned} y^p &= (\pm x + \sqrt{-C})((\pm x - \sqrt{-C}) \\ y^p &= (\frac{1}{2}(A + B\sqrt{-C}))^p(\frac{1}{2}(A - B\sqrt{-C}))^p \\ y^p &= \frac{1}{4}(A^2 + B^2C)^p, \end{aligned}$$

donc

$$y = \frac{1}{4}(A^2 + B^2C).$$

Mais cela ne peut se produire que si $p = 3$. En effet, identifions les parties imaginaires de (1.3.2), on trouve

$$2^p = B \sum_{r=0}^{r=\frac{p-1}{2}} \binom{p}{2r+1} A^{p-2r-1}(-B^2C)^r,$$

et comme B est impair alors $B = \pm 1$. Ainsi

$$\pm 2 \equiv \pm 2^p \equiv (-C)^{\frac{p-1}{2}} \equiv (-C \mid p) \equiv 0, \pm 1 (\mathrm{mod}\, p),$$

l'équation $\pm 2^p \equiv 0 (\mathrm{mod}\, p)$ ne peut pas se produire car p est impair, donc il reste à considérer l'équation $\pm 2^p \equiv \pm 1 (\mathrm{mod}\, p)$, mais $\pm 2^p \equiv 2 (\mathrm{mod}\, p)$ (petit theorème de Fermat) donc $p = 3$.

Identifions maintenant les parties réelles et les parties imaginaires de l'équation (1.3.2), on aura

$$\begin{aligned} \pm x &= \mathrm{Re}(\frac{1}{2}(A + \sqrt{-C}))^3, \\ 1 &= \mathrm{Im}(\frac{1}{2}(A + \sqrt{-C}))^3 \end{aligned}$$

ainsi

$$\begin{aligned} \pm 8x &= A^3 - 3AC \\ 8 &= 3A^2 - C, \end{aligned}$$

d'où le lemme suivant

Lemme 1.3.1 *La condition (1.3.2) se produit si et seulement si, on a*

$$C = 3A^2 \pm 8, \qquad p = 3 \qquad et \quad x = A^3 \pm A.$$

Le deuxième problème que Cohn a étudié est le problème des unités dans $\mathbb{Q}(\sqrt{-C})$. On sait que si $C \equiv 3(\mathrm{mod}\, 4)$, posons $C = 3d^2$, on a six unités, à savoir $\pm 1, \pm\omega, \pm\omega^2$ ou $\omega = \exp(i\frac{2\pi}{3})$. Dans ce cas, l'équation (1.3.2) admet une solution sauf si $p = 3$ et on aura

$$\pm x + d\sqrt{-3} = (\frac{1}{2}(A + Bd\sqrt{-3}))^3, \qquad A \equiv B(\mathrm{mod}\, 2). \tag{1.3.3}$$

Il s'ensuit de (1.3.3) le lemme suivant

Lemme 1.3.2 *Si $C = 3d^2$ alors on a $C = 48D^6,\ x = 4D^3,\ p = 3$.*

Le troisième problème est l'unicité de la factorisation dans l'anneau $\mathbb{Z}[\sqrt{-C}]$. Il y a neuf corps quadratiques imaginaires dans lesquels cette condition est satisfaite. Considérons par exemple les deux équations $x^2 + 74 = y^n$ et $x^2 + 85 = y^n$ avec x et y sont premiers entre eux et $n \geq 3$. Cohn a resolu ces deux équations pour n non multiple de 5, plus précisement, *Cohn* a prouvé que l'équation $x^2 + C = y^n$ avec n non multiple de 5 a pour solution $x = 13,\ y = 3, n = 3$ pour $C = 74$, et n'a pas de solutions pour $C = 85$. La raison pour laquelle Cohn a considéré la condition sur n est que le nombre de classes du corps qudratiques imaginaires $\mathbb{Q}(\sqrt{-C})$ est multiple de 5. Dans ce cas, on a pas unicité de la factorisation dans l'anneau $\mathbb{Z}[\sqrt{-C}]$. Rappelons que le nombre de classes mesure en quelque sorte la principalité d'un anneau, mais on peut contourner cette obstruction en faisant remarquer que l'idéal $\mathfrak{a}^5$ est principal pour tout $\mathfrak{a}$ dans $\mathbb{Z}[\sqrt{-C}]$ et n et 5 sont premiers entre eux, ce qu'a fait Cohn.

Dans [31], *Maurice Mignotte et Benjamin de Weger* ont résolu cette équation pour $n = 5$. Leur preuve est basée sur la théorie des approximations Diopahntiennes, en réduisant l'équation en une équation de *Thue* et en utilisant la théorie des formes linéaires en logarithmes, ils prouvent le résultat suivant

Théorème 1.3.1 *(Mignotte-Weger) L'équation Diopahntienne $x^2 + C = y^n$ où $C = 74$. (résp. $C = 85$) a les solutions suivantes $(x, y, n) = (13, 3, 5), (985, 99, 3)$. (résp. pas de solutions).*

Preuve. Voir [31] ■

Rappelons qu'une équation de *Thue* est une équation de la forme $f(X, Y) = m$ où f est un polynôme de deux variables irréductible de degré ≥ 3, et m entier relatif positif non nul.

Un résultat très important concernant les équations de *Thue* due à *Axel Thue* (1909) [42], il a démontré que si le polynôme homogène $f(X,Y) = \sum_{i=0}^{i=n} a_i X^i Y^{n-i}$ est irréductible dans $\mathbb{Q}[X,Y]$, une telle équation n'a qu'un nombre fini de solutions entières.

De même pour certaines valeurs de C où le $h_{\mathbb{Q}(\sqrt{-C})}$ n'est pas toujours égal à 1, mais l'essentiel est que $p \nmid h_{\mathbb{Q}(\sqrt{-C})}$.

Dans notre équation principale $h_{\mathbb{Q}(\sqrt{-13})} = 2$, nous voyons par la suite que l'idéal $(\pm x + \sqrt{-13}) = \mathfrak{a}^3$ et comme $h_{\mathbb{Q}(\sqrt{-13})}$ est premier avec 3, alors $\mathfrak{a}^3$ doit être principal.

Le problème le plus surieux dans l'étude de *Cohn* en résolvant l'équation $x^2 + C = y^n$, réside dans le cas où les deux facteurs $(\pm x + \sqrt{-C})$ et $(\pm x - \sqrt{-C})$ ont un facteur commun. Soit par exemple l'équation

$$x^2 + 7 = y^n,\ n \geq 3$$

où x est impair, si l'on factorise, on aura

$$(\pm x + \sqrt{-7})(\pm x - \sqrt{-7}) = y^n,$$

mais les deux facteurs $(\pm x + \sqrt{-7}), (\pm x - \sqrt{-7})$ sont divisibles par $\frac{1}{2}(1 + \sqrt{-7})$ et $\frac{1}{2}(1 - \sqrt{-7})$. En effet, prenons d'abord x impair ce qui implique que y^n est pair. Dans ce cas la norme de $\frac{1}{2}(1 + \sqrt{-7})$ vaut 2 qui divise la norme y^n, donc $\frac{1}{2}(1 + \sqrt{-7})$ divise y^n ce qui implique que $\frac{1}{2}(1 + \sqrt{-7})$ est un diviseur commun de $(\pm x + \sqrt{-7})$ et $(\pm x - \sqrt{-7})$. La méthode de *Cohn* est inapplicable à la résolution de l'équation $x^2 + 7 = y^n$, *Ramanujan* [32] a proposé l'équation qui porte son nom en posant $y = 2$. Ce cas particulier a été résolu complètement par *Negell*. *Cohn* a conjucturé que l'équation(**??**) a les mêmes solutions que celles de *Ramanujan-Negell*. En 1997, *Mahoue* [43] a donné les deux résultas : cette équation n'a pas de solutions pour y impair et que pour $2 \mid y$, l'ensemble des solutions est fini et satisfait $n < 5.10^6$ et $y < \exp\exp\exp 30$, dans la même année, *Lesage* [25] a amélioré ce résultat, en particulier si (x, y, n) est une solution de l'équation $x^2 + 7 = y^n$ alors $n \leq 6.6 \times 10^{15}$ en utilisant la théorie des formes linéaires en logarithmes.

En 2003, *Siksek et Cremona* [34] ont étudié l'équation, ils ont prouvé en utilisant des méthodes plus sophistiqués telles que les courbe de *Frey*, le théorème de *Ribet* et l'approche

modulaire que l'équation n'a pas de solution si n est composé et $n > 15$, ainsi qu'avec n premier compris entre $11 \leq n \leq 10^8$.

Théorème 1.3.2 *(Siksek, Cremona) L'équation $x^2 + 7 = y^p$, n'a pas de solution avec p premier et $11 \leq p \leq 10^8$.*

Preuve. Voir [34]. ■

Récemment, *Mignotte, Siksek et Bugeaud* ont démontré la conjecture de *Cohn* sur cette équation [9].

Enfin, pour le cinquième point, supposons que C est sans facteurs carrés et posons $C = cd^2$ avec c n'est pas un carré parfait. Si $c \equiv 1, 2 (\mathrm{mod}\, 4)$ on aura

$$\pm x + d\sqrt{-c} = (a + b\sqrt{-c})^p, \tag{1.3.4}$$

et si Si $c \equiv 3 (\mathrm{mod}\, 4)$, on obtient

$$\pm x + d\sqrt{-c} = (\frac{1}{2}(A + B\sqrt{-c})^p) \qquad A \equiv B \equiv 1 (\mathrm{mod}\, 2). \tag{1.3.5}$$

L'équation (1.3.4) nous donne en identifiant les parties imaginaires de ses cotés

$$d = b \sum_{r=0}^{r=\frac{p-1}{2}} \binom{p}{2r+1} a^{p-2r-1}(-b^2c)^r,$$

si $b = \pm d$, on se ramène à l'équation (1.3.1), sinon pour chaque valeur de b, il existe un nombre fini de p satisfaisant (1.3.4) car

$$d/b \equiv 0, 1 \ et \ -1 (\mathrm{mod}\, p).$$

Dans l'équation (1.3.5), nous remarquons que si $(\frac{1}{2}(A+B\sqrt{-c})^p) \in \mathbb{Z}[\sqrt{-c}]$ alors, d'aprés le lemme (1.3.2) $c \equiv 3 (\mathrm{mod}\, 8)$, et $p = 3$, ainsi

$$\pm x = (\frac{1}{2}(A + B\sqrt{-c})^3,$$

en identifiant les parties réelles, on trouve

$$\pm x = \frac{1}{8}(A^3 - 3AB^2c).$$

Après cette étude, nous voyons bien l'importance et la nécessité de l'unicité de la factorisation dans le théorème de *Cohn* suivant :

Théorème 1.3.3 *(Cohn) Soit $C > 0$, $C = cd^2$, c n'est pas un carré parfait, $c \not\equiv 7 (\mathrm{mod}\, 8)$. Si p un nombre premier impair et si $x^2 + C = y^p$, pour $p \gcd(x, y) = 1$, alors soit,*

1) il existe deux entiers a, b avec $b \mid d$, $y = a^2 + b^2 C$ et $\pm x + d\sqrt{-c} = (a + b\sqrt{-c})^p$,

2) $C = 3A^2 \pm 8, \qquad p = 3 \qquad et \quad x = A^3 \pm A$,

3) $C = 48D^6, x = 4D^3, p = 3$,

4) $p \mid h_{\mathbb{Q}(\sqrt{-c})}$,

5) $C \equiv 3 (\mathrm{mod}\, 8)$, $p = 3$, et il existe deux entiers A, B avec $B \mid d$, $y = \dfrac{1}{4}(A^2 + B^2 c)$, $\pm x + d\sqrt{-c} = \dfrac{1}{8}(A + B\sqrt{-c})^3$,

Preuve. Voir [13], [16]. ■

1.4 Conclusion

Vu de ces difficultiés, *Cohn* a pu résoudre l'équation (0.0.3) que pour 77 valeurs de $C \leq 100$, satisfaisants les conditions cités dans le théorème (1.3.3). Ses résultats sont donnés dans le théorème ci-dessous

Théorème 1.4.1 *(Cohn) Pour $C \in \{$ 1, 3, 5, 6, 8, 9, 10, 14, 21, 22, 24, 27, 29, 30, 33, 34, 36, 37, 38, 41, 42, 43, 46, 50, 51, 52, 57, 58, 59, 62, 66, 68, 69, 70, 73, 75, 78, 82, 84, 85, 88, 90, 91, 93, 94, 98$\}$, l'équation (0.0.3) n'admet pas de solutions. Dans les autres cas, on a*

$$\begin{aligned}(C, x, y, n) \;=\; & (2,5,3,3), (4,2,2,3), (4,11,5,3), (11,4,3,3), (11,58,15,3), (12,2,2,4),\\ & (13,70,17,3), (16,4,2,5), (17,8,3,4), (19,18,7,3), (19,22434,55,5),\\ & (20,14,6,3), (26,1,3,3), (26,207,35,3), (32,7,3,4), (32,88,6,5),\\ & (35,36,11,3), (40,52,14,3), (44,9,5,3), (48,8,2,6), (48,148,56,3),\\ & (49,24,5,4), (49,524,65,3), (53,26,3,6), (53,156,29,3), (54,17,7,3),\\ & (56,5,3,4), (56,76,54,3), (61,8,5,3), (64,64,2,7), (65,4,3,4),\\ & (67,110,23,3), (76,49,5,3), (76,1015,101,3), (77,2,3,4), (80,1,3,4),\\ & (81,46,13,3), (83,140,3,9), (89,6,5,3), (96,23,5,4), (97,48,7,4).\end{aligned}$$

Preuve. Voir [13], [16]. ■

Chapitre 2

Résolution de l'équation Diophantienne $x^2 + 13^k = y^n,\ n \geq 3.$

2.1 Introduction

Plusieurs cas de l'équation Diophantienne de la forme $x^2 + q^k = y^n$, où q est premier et x, y, k et n sont des entiers ont été étudiés dans les dernières années. Lorsque $q = 2$, et k est impair, *Cohn* [14] a prouvé que cette dernière admet trois familles de solutions. Pour $q = 3$ et k est impair, *Arif et Abu Muriefah* [1] ont prouvé que cette équation a une seule famille de solutions et *Luca* [29] a montré l'existence d'une famille de solutions pour $q = 3$ et m est un entier pair. *Arif et Abu Muriefah* ont prouvé que l'équation $x^2 + q^{2k+1} = y^n$ où q est premier impair vérifiant $q \not\equiv 7 \bmod 8$ et n impair, $n \geq 5$ tel que n n'est pas divisible par 3 et $\text{pgcd}(n, h_{\mathbb{Q}(\sqrt{-q})}) = 1$ où $h(\sqrt{-q})$ est le nombre de classe du corps de nombres $\mathbb{Q}(\sqrt{-q})$ a exactement deux familles de solutions qui sont

$$\begin{aligned} q &= 19,\ x = 22434.19^{5M},\ y = 55.19^{2M},\ k = 5M,\ n = 5, \\ q &= 341,\ x = 2759646.341^{5M},\ y = 377.341^{2M},\ k = 5M,\ n = 5 \end{aligned}$$

.

Dans [20], *Hui li zhu et MaoHua Le* ont donné toutes les solutions de certaines équations de Ramanujan- Negell de la forme

$$x^2 + q^m = y^n, \quad n \geq 3 \quad \text{et } q \in \{11, 19, 43, 67, 163\},$$

où $h_{\mathbb{Q}(\sqrt{-q})} = 1$, ils ont prouvé le résultat suivant

Proposition 2.1.1 *Toutes les solutions de l'équation*

$$x^2 + q^m = y^n, \quad n \geq 3 \quad \text{et } q \in \{11, 19, 43, 67, 163\},$$

sont

$$\begin{aligned}
q &= 11,\ x = 2.11^{3M},\ y = 5.11^{2M},\ m = 6M+3,\ n = 3,\\
q &= 11,\ x = 4.11^{3M},\ y = 3.11^{2M},\ m = 6M+1,\ n = 3,\\
q &= 11,\ x = 58.11^{3M},\ y = 15.11^{2M},\ m = 6M+1,\ n = 3,\\
q &= 11,\ x = 9324.11^{3M},\ y = 443.11^{2M},\ m = 6M+3,\ n = 3,\\
q &= 19,\ x = 18.19^{3M},\ y = 7.19^{2M},\ m = 6M+1,\ n = 3,\\
q &= 19,\ x = 22434.19^{5M},\ y = 55.19^{2M},\ m = 10M+3,\ n = 5,\\
q &= 67,\ x = 110.67^{3M},\ y = 23.67^{2M},\ m = 6M+1,\ n = 3,
\end{aligned}$$

où M est un entier positif.

Dans ce chapitre, on va résoudre complétement l'équation Diophantienne (0.0.2) où $n \geq 3$, et $k \in \mathbb{N}$, [18] en particulier, la résolution de (0.0.2) pour $n = 3$ qui n'a pas été traité dans [1], ainsi pour le cas où k est pair. En utilisant la théorie algébrique des nombres introduite dans le chapitre 1 et une nouvelle théorie sur les nombres de *Lucas*.

2.2 Pairs de Lucas.

2.2.1 Définitions et notations

Suite récurrente binaire

Définition 2.2.1 *Soit k un entier ≥ 1. Une suite $(u_n)_{n\geq 0} \subset \mathbb{C}$ est dite linéairement récurrente d'ordre k si la rcurrence*

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + ... + a_k u_n$$

est satisfaite pour tout $n \geq 0$, pour certains coefficients $a_1, ..., a_k \in \mathbb{C}$.

Le polynôme $f \in \mathbb{C}[X]$ défini par

$$f(X) = X^k - a_1X^{k-1} - ... - a_k \in \mathbb{C}[X]$$

est dit polynôme caractéristique de la suite $(u_n)_{n\geq 0}$.

Proposition 2.2.1 *Supposons que $f(X) \in \mathbb{Z}[X]$ a des racines distinctes $\alpha_1, ..., \alpha_k$. Il existe alors des constantes $c_1, ..., c_k \in K = \mathbb{Q}(\alpha_1, ..., \alpha_k)$ telles que*

$$u_n = \sum_{i=1}^{k} c_i\alpha_i^n$$

est satisfaite pour tout $n \geq 0$.

Si $k = 2$, la suite $(u_n)_{n\geq 0}$ est dite suite récurrente binaire. Dans ce cas, son polynôme caractéristique est donné par la formule

$$\begin{aligned} f(X) &= X^2 - a_1X - a_2 \\ &= (X - \alpha_1)(X - \alpha_2) \end{aligned}$$

Supposons que $\alpha_1 \neq \alpha_2$. La proposition précédente nous donne

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n \quad \text{pour tout } n \geq 0.$$

Définition 2.2.2 *La suite récurrente binaire $(u_n)_{n\geq 0}$ donnée par la formule ci- dessus est dite non dégénérée si $c_1c_2\alpha_1\alpha_2 \neq 0$ et α_1/α_2 n'est pas une racine de l'unité.*

Suite récurrente binaire associée à l'équation de *Pell*

Soit d un entier > 1 qui n'est pas un carré parfait et soit (x_1, y_1) la solution minimale en entiers positifs de l'équation

$$x^2 - dy^2 = \pm 1. \tag{2.2.1}$$

On pose

$$\zeta = x_1 + \sqrt{d}y_1 \quad \text{et} \quad \eta = x_1 - \sqrt{d}y_1$$

On sait que toutes les solutions de l'équation (2.2.1) sont données par la forme $(x, y) = (x_l, y_l)$ pour un certain entier l, où

$$x_l + \sqrt{d}y_l = (x_1 + \sqrt{d}y_1)^l = \zeta^l,$$

et

$$x_l - \sqrt{d}y_l = (x_1 - \sqrt{d}y_1)^l = \eta^l.$$

on conclut donc que

$$x_l = \frac{\zeta^l + \eta^l}{2} \quad \text{et} \quad y_l = \frac{\zeta^l - \eta^l}{2\sqrt{d}} \quad \text{pour tout } l \geq 1. \tag{2.2.2}$$

Si on pose $(x_0, y_0) = (1, 0)$, donc la formule (2.2.2) est satisfaite aussi pour $l = 0$.

Il est facile de vérifier que les suites $(x_l)_{l\geq 0}$ et $(y_l)_{l\geq 0}$ sont des suites récurrentes binaires de polynôme caractéristique

$$\begin{aligned} f(X) &= X^2 - a_1X - a_2 \\ &= (X - \zeta)(X - \eta) \\ &= X^2 - (\zeta + \eta)X + \zeta\eta \\ &= X^2 - 2x_1X \pm 1. \end{aligned}$$

Suite de Lucas

Définition 2.2.3 *Une suite de Lucas du premier type $(u_n)_{n\geq 0}$ est une suite récurrente binaire avec $u_0 = 0$ et $u_1 = 1$ est telle que a_1 et a_2 sont premiers entre eux.*

Une suite de Lucas du second type $(u_n)_{n\geq 0}$ est une suite récurrente binaire avec $u_0 = 2$ et $u_1 = 1$ et telle que a_1 et a_2 sont premiers entre eux.

Autrement dit, une suite de Lucas du premier type $(u_n(P, Q))_{n\geq 0}$ où P, Q sont des entiers naturels est définie par $u_0 = 1$, $u_1 = 1$ et pour tout $n > 1$, $u_{n+1} = Pu_n - Qu_{n-1}$.

Pour la suite de Lucas du second type, nous gardons la même définition en prenant $u_0 = 2$.

Remarque 2.2.1 *Les deux types des suites de Lucas ont le même polynôme caractéristique.*

Si α_1 et α_2 sont les racines du polynôme caractéristique d'une suite de Lucas du premier type (résp. du second type), alors le terme général de $(u_n(P, Q))_{n\geq 0}$ est donné par

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2} \quad \text{pour tout } n \geq 0. \ (\textit{résp. } u_n = \alpha_1^n + \alpha_2^n).$$

En effet, Soit α_1, α_2 les racines de polynôme caractéristique de la suite de Lucas de premier type $(u_n)_{n\geq 0}$. On a $\alpha_1 \neq \alpha_2$, et pour tout $n \geq 0$,il existe $c_1, c_2 \in \mathbb{Q}(\alpha_1, \alpha_2)$ tels que

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n$$

or $u_0 = 0$ ce qui nous donne $c_1 = -c_2$ et $u_1 = 1$ donc $c_1 = \dfrac{1}{\alpha_1 - \alpha_2}$, alors pour tout $n \geq 0$, on a

$$u_n = c_1(\alpha_1^n - \alpha_2^n),$$

ce qui implique que

$$u_n = \frac{\alpha_1^n - \alpha_2^n}{\alpha_1 - \alpha_2}.$$

Pour les suites de Lucas de second type, on a $u_0 = 2$ donc $c_2 = 2 - c_1$, et $u_1 = 1$ alors $c_1 = \dfrac{1 - 2\alpha_2}{\alpha_1 - \alpha_2}$ et $c_2 = \dfrac{2\alpha_1 - 1}{\alpha_1 - \alpha_2}$. Et comme le polynôme caractéristique de la suite de Lucas est donné par

$$P(X) = X^2 - X + 1,$$

alors on conclut que $\alpha_1 + \alpha_2 = 1$ et $\alpha_1\alpha_2 = 1$, ce qui implique

$$c_1 = c_2 = 1,$$

donc pour tout $n \geq 0$, on a

$$u_n = \alpha_1^n + \alpha_2^n.$$

Exemple 2.2.1 *Soit (x_l, y_l) la $l^{ième}$ solution de l'équation de Pell $x^2 - dy^2 = \pm 1$, donc on a*

$$\frac{y_l}{y_1} = \frac{\zeta^l - \eta^l}{2\sqrt{d}y_1} = \frac{\zeta^l - \eta^l}{\zeta - \eta}$$

ainsi la suite $(y_l/y_1)_{l\geq 0}$ est aussi une suite de Lucas du premier type.

De même, on a

$$x_l = \frac{\zeta^l + \eta^l}{2},$$

donc la suite de terme général $(2x_l)_{l\geq 0}$ est une suite de Lucas du second type.

Facteurs premiers de termes d'une suite de Lucas

Dans la suite, soit $(u_n)_{n\geq 0}$ est une suite de Lucas. Posons $\Delta = (\alpha_1 - \alpha_2)^2$.

Proposition 2.2.2 *Soit p un nombre premier. On a les propriétés suivantes*

(i) *Si $p \mid a_2$, alors $p \nmid u_n$ pour tout $n \geq 1$,*

(ii) *si $p \mid \Delta$, alors $p \mid u_p$,*

(iii) *si $p \nmid \Delta a_2$ et $(\Delta \mid p) = 1$, alors $p \mid u_{p-1}$,*

(iv) *si p ne satisfait pas (i) et (iii), alors $p \mid u_{p+1}$.*

Définition 2.2.4 *Un facteur premier p de u_n est dit primitif pour u_n si $p \mid u_n$ et $p \nmid \Delta.u_1...u_{n-1}$.*

Paires de Lucas

Définition 2.2.5 *Une Paire de Lucas est une paire d'entiers algébriques (α, β) telles que $\alpha+\beta$ et $\alpha\beta$ soient des entiers relatifs premiers entre eux et $\dfrac{\alpha}{\beta}$ n'est pas une racine de l'unité. Pour chaque paire (α, β) de Lucas, on lui associe la suite de Lucas du premier type définie ci-dessus.*

Définition 2.2.6 *Une paire (α, β) de Lucas est dite n-défectueuse si et seulement si $u_n(\alpha, \beta)$ n'a aucun diviseur primitif.*

Théorème du diviseur primitif

Avant d'énoncer le théorème du diviseur primitif d'un terme d'une suite de Lucas, developpé par Bilu, Harnot et Voutier, il est nécessaire d'énoncer le résultat de *Carmichael* [10] suivant

Théorème 2.2.1 *Soit $(u_n)_{n\geq 0}$ une suite de Lucas. Si $n > 12$, alors aucun terme u_n n'a un diviseur primitif.*

Preuve. Voir [10]. ■

Maintenant, on va énoncer la version forte du théorème. [7], [28].

Théorème 2.2.2 *Soit n un entier tel que $4 < n \leq 30$ et $n \neq 6$, alors toutes paires de Lucas sous la forme*

$$\Big((a - \sqrt{b})/2, (a_1 + \sqrt{b})/2), n\Big)$$

est $n-$défectueuse où (a, b, n) est l'un des triplets suivants

n	(a, b)
5	$(1,5),(1,-7),(2,-40),(1,-11),(1,-15),(12,-76),(12,-1364)$
7	$(1,-7),(1,-19)$
8	$(2,-24),(1,-7)$
10	$(2,-8),(5,-3)$
12	$(1,5),(1,-7),(1,-11),(2,-56),(1,-15),(1,-19)$
13	$(1,-7)$
18	$(1,-7)$
30	$(1,-7)$

(2.2.3)

Preuve. Voir [7], [28]. ■

Proposition 2.2.3 *Toute paire de Lucas est 1-défectueuse.*

Après avoir defini tous les outils essentiels pour résoudre notre équation, nous calculons le nombre de classes d'idéaux du corps $\mathbb{Q}\left(\sqrt{-13}\right)$ en utilisant la proposition (1.2.8).

Calcul du nombre de classes du corps $\mathbb{Q}(\sqrt{-13})$

Le nombre de classes du corps $\mathbb{Q}(\sqrt{-13})$ est égal au nombre de solutions du système d'équations

$$\begin{cases} b^2 - 4ac = D_{\mathbb{Q}(\sqrt{-13})} \\ a \leq \sqrt{-D_{\mathbb{Q}(\sqrt{-13})}/3}. \\ -a < b \leq a < c \text{ ou } 0 \leq b \leq a = c. \end{cases}$$

où $D_{\mathbb{Q}(\sqrt{-13})}$ est le discriminant du corps $\mathbb{Q}(\sqrt{-13})$, puisque $-13 \equiv 3 (\mathrm{mod}\, 4)$ alors $D_{\mathbb{Q}(\sqrt{-13})} = 4(-13) = -52$. Donc le système devient

$$\begin{cases} b^2 - 4ac = -52, \\ a \leq \sqrt{17.33}, \\ . - a < b \leq a < c \text{ ou } 0 \leq b \leq a = c. \end{cases}$$

et comme $a \in \mathbb{N} - \{0\}$ alors $a \in \{1, 2, 3, 4\}$.

- Le cas $0 \leq b \leq a = c$ pour toutes valeurs de $a \in \{1, 2, 3\}$, ne peut se produire car $b^2 < 0$.

Si $a = c = 4$, alors on trouve $b^2 = 12$, ce qui est impossible.

Il nous reste le cas où b prend les valeurs $0, \pm 1, \pm 2$ et ± 3.

- Si $b = 0$, pour tout $a \in \{1, 2, 3, 4\}$, alors il n'existe pas de valeur de c.

- Le cas $b = \pm 1$ mène à $4ac = 53$, ce qui est impossible.

- Le cas $b = \pm 2$ mène à $ac = 13$, si $a = 1$ on obtient $c = 13$. Pour les autres valeurs de a, il n'existe pas de valeurs de c qui vérifient l'équation $ac = 13$.

- Le cas $b = \pm 3$ mène à $4ac = 61$, ce qui est impossible.

- Le cas $b = \pm 4$ mène à $2ac = 33$, ce qui est impossible.

Donc les seules solutions du système sont $(a, b, c) = (1, \pm 2, 13)$, donc $h(\mathbb{Q}(\sqrt{-13})) = 2$.

2.3 Résultats principaux

Dans cette section nous allons donner toutes les solutions de l'équation (0.0.3). Pour cela, nous avons besoin des résultats suivants [33] , [11]

Lemme 2.3.1 *(Nagell) Soit n un entier positif ≥ 3, l'équation Diophantienne $3x^2+1 = y^n$, n'a pas de solutions en entiers positifs x et y.*

Preuve. Voir [33]. ■

Lemme 2.3.2 *(Catalan) L'équation Diophantienne $x^m - y^n = 1$ a une seule solution en entiers positifs $(x, y, m, n) = (3, 2, 2, 3)$.*

Preuve. Voir [11],[12]. ■

2.3.1 Résolution de l'équation Diophantienne $3x^2 + 1 = 13^y$.

Ce résultat est utile lors pour la résolution de l'équation (0.0.3).

Théorème 2.3.1 *L'équation Diophantienne*

$$3x^2 + 1 = 13^y \tag{2.3.1}$$

où $x, y > 0$, a une seule solution en entiers positifs $(x, y) = (2, 1)$.

Preuve. Cas 1 : y est impair.

Pour $y \geq 3$ impair, l'équation $3x^2 + 1 = 13^y$ n'a pas de solutions en nombres entiers strictement positifs. (Lemme 2.3.1).

Pour $y = 1$, l'équation a une solution $(x, y) = (2, 1)$.

- Cas 2 : y est pair.

Posons $y = 2t$ où $t > 0$, l'équation (3.3.1) devient $13^{2t} - 3x^2 = 1$. Posons

$$X = 13^t \quad \text{et } Y = x,$$

notre équation devient $X^2 - 3Y^2 = \pm 1$. C'est une équation de *Pell* avec la solution minimale $(X_1, Y_1) = (2, 1)$ et la seconde solution est $(X_2, Y_2) = (7, 4)$. Donc les solutions de l'équation $X^2 - 3Y^2 = \pm 1$ sont données par

$$(X_l, Y_l) = (\frac{\epsilon^l + \varsigma^l}{2}, \frac{\epsilon^l - \varsigma^l}{2\sqrt{3}}), \quad \text{avec } \epsilon = 2 + \sqrt{3} \text{ et } \varsigma = 2 - \sqrt{3}.$$

■

Lemme 2.3.3 *La suite du terme général $u_l = 2X_l$ pour tout $l \geq 0$, est une suite de Lucas du second type.*

Preuve. Pour tout $l \geq 0$, $u_l = \epsilon^l + \varsigma^l$, $u_0 = 2$ et $u_1 = 4$.

Le polynôme caractéstique de la suite (u_l) est

$$P(x) = x^2 - 4x + 1$$

donc $P = 4$ et $Q = 1$, alors pour tout $l > 1$, $u_l = 4u_{l-1} - u_{l-2}$ qui est une suite de Lucas du second type. ■

Revenons à notre preuve, appliquons le théorème du diviseur primitif de *Carmicheal* (théorème 2.2.2), il en suit que si $l > 12$ alors le terme u_l a un facteur premier $p \equiv \pm 1 (\mathrm{mod}\, l)$.

En particulier u_l ne peut pas être une puissance de 13 si $l > 12$. Pour $l \leq 12$ on obtient les valeurs suivantes:

l	3	4	5	6	7	8	9	10	11	12
u_l	52	194	724	2702	10 084	37 634	140 452	524 174	1956 244	7300 802

Par une simple vérification, on voit que ses valeurs ne sont pas des puissances de 13, donc X_l n'est pas une puissance de 13 pour tout $l \leq 12$. On conclut que l'équation (2.3.1) n'a pas de solutions entiers. Ce qui achève la preuve.

2.3.2 Résolution de l'équation Diophantienne $x^2+13^{2m} = y^n$, $n \geq 3$.

La deuxième équation Diophantienne qu'on a résolu est la suivante

Théorème 2.3.2 *Soit m un entier positif, l'équation Diophantienne (0.0.5) n'a pas de solutions en entiers positifs .*

Preuve. Supposons que $p\gcd(x, y) = 1$.

Soit $k = 2m$, avec $m > 0$. Si x est impair , alors y est pair et on obtient $x^2 + 13^{2m} \equiv 2 \bmod(8)$, mais $y^n \equiv 0(\bmod 8)$ ceci est impossible, alors x est pair et y est impair.

- Cas 1: $n = 3$

Factorisons l'équation (0.0.5) dans $\mathbb{Z}[i]$, on obtient

$$(x + 13^m i)(x - 13^m i) = y^3$$

Passant aux idéaux de $\mathbb{Z}[i]$, on trouve

$$\langle x + 13^m i\rangle \langle x - 13^m i\rangle = \langle y\rangle^3$$

Puisque x et y sont premiers entre eux et $13^{2m} \equiv 1(\bmod 4)$, on obtient x est pair. Mais les idéaux $\langle x + 13^m i\rangle$ et $\langle x - 13^m i\rangle$ sont premiers entre eux dans $\mathbb{Z}[i]$. En effet, soit P un idéal premier divisant à la fois $\langle x + 13^m i\rangle$ et $\langle x - 13^m i\rangle$, alors $\langle x + 13^m i\rangle \in P, \langle x - 13^m i\rangle \in P$, $2x \in P$, donc $P \mid \langle 2x\rangle$, et $P \mid \langle y\rangle$, car il intervient dans la décomposition de $\langle y\rangle^3$ en produit d'idéaux premiers. Passant aux normes, il vient $N(P) \mid N(2x) = 4x^2$, $N(P) \mid N(y) = y^2$. Puisque y est impair, $N(P)$ est impair, d'où $N(P) \mid x^2$ et $N(P) \mid y^2$, or $\langle P\rangle \neq \langle 1\rangle$, donc

$N(P) \neq 1$, et x, y ont un diviseur commun différent de 1, contradiction du fait que x et y sont premiers entre eux. Dans $\mathbb{Z}[i]$ qui est un anneau de Dedekind (Propriété de factorisation) (Voir Théorème (1.2.2)), alors les deux facteurs à gauche sont des cubes d'éléments de $\mathbb{Z}[i]$, (les unités de $\mathbb{Z}[i]$ sont $\pm 1, \pm i$), alors

$$\begin{cases} x + 13^m i = (u + iv)^3 \\ x - 13^m i = (u - iv)^3 \end{cases}$$

Pour certains entiers non nuls u et v premiers entre eux. On trouve

$$2.13^m i = (u + iv)^3 - (u - iv)^3$$

ceci implique que

$$13^m = v(3u^2 - v^2)$$

or u et v sont premiers entre eux, en effet, soit p un facteur premier commun de u et v, alors p divise x et y qui est impossible, car

$$\begin{cases} x = u(u^2 - 6v^2) \\ y = u^2 + v^2 \end{cases}$$

alors $v = \pm 1$ ou $v = \pm 13^m$ ce qui est implique

$$\begin{cases} 3u^2 = 1 \pm 13^m \\ 3u^2 = \pm 1 + 13^{2m} \end{cases}$$

L'équation $3u^2 = 1 - 13^m$ n'a pas de solutions en entiers positifs (évident).

L'équation $3u^2 = 1 + 13^m$ n'a pas de solutions en entiers positifs, puisque $1 + 13^m$ est congru à 2 modulo 3 et $3u^2 \equiv 0 (\mathrm{mod}\, 3)$.

De même, l'équation $3u^2 = 1 + 13^{2m}$ n'a pas de solutions en entiers positifs, puisque $1 + 13^{2m}$ est congru à 2 modulo 3 et $3u^2 \equiv 0 (\mathrm{mod}\, 3)$.

Il nous reste l'équation $3u^2 = -1 + 13^{2m}$ qui est impossible. (Théorème 2.3.1).

- Cas 2 : $n = 4$

L'équation (3.3.2) implique

$$(y^2 + x)(y^2 - x) = 13^{2k}$$

Puisque x est pair et y est impair alors $y^2 + x$ et $y^2 - x$ sont premiers entre eux, ce qui implique que

$$\begin{cases} y^2 + x = 13^{2k} \\ y^2 - x = 1 \end{cases}$$

qui nous conduit à

$$13^{2k} - 2y^2 = -1$$

c'est une équation de Pell $X^2 - 2y^2 = \pm 1$ avec $X = 13^k$.

La solution minimale de cette équation est $(X_1, y_1) = (1, 1)$, la seconde est $(X_2, y_2) = (3, 2)$ et la troisième est $(X_3, y_3) = (7, 5)$, et pour tout $l \geq 1$; X_l est donné par

$$X_l = \frac{\zeta^l + \eta^l}{2}$$

où $\zeta = 1 + \sqrt{2}$ et $\eta = 1 - \sqrt{2}$ est une suite de Lucas du second type. Par le théorème du diviseur primitif de Carmicheal (Théorème 2.2.2) , il s'en suit que si $l > 12$ alors X_l a un facteur premier $p \equiv \pm 1(\mod l)$. En particulier X_l ne peut pas être une puissance de 13 si $l > 12$. Pour $l \leq 12$, on obtient les valeurs suivantes:

l	3	4	5	6	7	8	9	10	11	12
X_l	7	17	41	99	239	577	1393	3363	8119	19 601

qui ne sont pas des puissances de 13.

-Cas 3: $n \geq 5$.

Soit (x, y, m, n) une solution de l'équation (3.3.2) et d un diviseur de n, alors $(x, y^{\frac{n}{d}}, m, d)$ est aussi une solution de (3.3.2). Les cas où $d = 3$ ou $d = 4$ sont résolus précédemment. Comme n est premier avec 3 et 4, donc il existe un nombre premier $p \geq 5$ qui divise n. Alors, on a:

$$(x + 13^m i)(x - 13^m i) = y^p,$$

passant en termes d'idéaux, on trouve

$$\langle x + 13^m i \rangle \langle x + 13^m i \rangle = \langle y^p \rangle .$$

Mais les idéaux $\langle x + 13^m i \rangle$ et $\langle x - 13^m i \rangle$ sont premiers entre eux dans $\mathbb{Z}[i]$ (même argument). Comme p est impair et les unités de $\mathbb{Z}[i]$ d'ordre divisant 4, on conclut qu'il existe des entiers relatifs non nuls u et v premiers entre eux. En effet, soit l un diviseur premier de u et v, donc l doit diviser x et y, contradiction du fait que le $p\gcd(x, y) = 1$. Ainsi, si on pose $\alpha = u + iv$, alors

$$\begin{cases} x + 13^m i = \alpha^p \\ x - 13^m i = \overline{\alpha}^p \end{cases},$$

on aura

$$\frac{13^m}{v} = \frac{\alpha^p - \overline{\alpha}^p}{\alpha - \overline{\alpha}},$$

Posons

$$u_n = \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}, \quad n \geq 0.$$

■

Lemme 2.3.4 *La suite* $\{u_n\}_{n\geq 0}$ *de terme général* $u_n = \dfrac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}$ *pour tout* $n \geq 0$ *est une suite de Lucas, et en plus l'entier* u_n *est sans diviseur primitif.*

Preuve. Tout d'abord, il est facile de voir que (u_n) est une suite de Lucas du premier type. Montrons maintenant que $(\alpha, \overline{\alpha})$ est une paire de Lucas.

Comme

$$\begin{cases} x + 13^m i = \alpha^p \\ x - 13^m i = \overline{\alpha}^p \end{cases},$$

alors

$$\alpha^p.\overline{\alpha}^p = x^2 + 13^{2m} = y^p,$$

donc

$$\alpha.\overline{\alpha} = y,$$

de plus $(\alpha + \overline{\alpha}) = 2u \in \mathbb{Z}$. Soit p un diviseur premier commun de $(\alpha + \overline{\alpha})$ et $\alpha.\overline{\alpha}$, alors p divise $2u$ et p divise y. Mais p est premier donc p divise u et y. Comme $y = u^2 + v^2$ alors p doit diviser $v^2 = y - u^2$, donc p divise v, contradiction du fait que u, v sont premiers entre eux. Il nous reste à montrer que $\dfrac{\alpha}{\overline{\alpha}}$ n'est pa une racine de l'unité. En effet les racines de l'anneau $\mathbb{Z}[i]$ sont $\pm 1, \pm\sqrt{-1}$. Posons $\dfrac{\alpha}{\overline{\alpha}} = \xi$, avec $\xi \in \{\pm 1, \pm\sqrt{-1}\}$. Si $\xi = \pm 1$, on aura

$$\begin{cases} u^2 - v^2 = \pm(u^2 + v^2) \\ 2uv = 0 \end{cases},$$

donc $u = 0$ ou $v = 0$ (impossible), ainsi $\dfrac{\alpha}{\overline{\alpha}}$ ne peut pas être une racine de l'unité. Posons maintenant $\xi = \pm 1$, dans ce cas, on aura

$$\begin{cases} u^2 - v^2 = 0 \\ (u \pm v)^2 = 0 \end{cases},$$

les deux équations nous donnent $u = \pm v$: impossible sauf si $u = \pm v = \pm 1$ car u et v sont premiers entre eux . Dans le cas où $u = \pm v = \pm 1$, on aura

$$\pm 13^m = \frac{(1+i)^n - (1-i)^n}{2i}$$

et les autres cas sont analogues à celle ci. Ce qui nous conduit à

$$\pm 13^m = \begin{cases} 0 & si \quad n \equiv 0 (\mathrm{mod}\, 4), \\ (-2)^{\left[\frac{n}{2}\right]} & \text{sinon} \end{cases}$$

où [.] désigne la partie entière. On voit que les seules valeurs de n pour lesquelles $(-2)^{\left[\frac{n}{2}\right]}$ est une puissance de 13 est $n = 0, 1$. Ce qui est impossible car $n \geq 3$.

Alors on conclut que $(\alpha, \overline{\alpha})$ est une paire de lucas.

Par l'extension du théorème du diviseur primitif de *Carmichael* des suites de Lucas avec les racines conjuguées par *Bilu, Hanrot et Voutier* (Théorème 2.2.3), on sait que si $p > 30$ est premier, alors u_p doit avoir un diviseur $q \equiv \pm 1 (\mathrm{mod}\, p)$. En particulier, u_p ne peut pas être une puissance de 13 pour chaque p.

Pour $p = 5$, les seules pairs de Lucas sans diviseurs primitifs sont données par les valeurs apparues dans le tableau (2.2.2) dans théorème (2.2.3) [6], les seuls pairs de Lucas sans diviseurs primitifs sont $\alpha = 1 \pm 10i$, $6 \pm 19i$ et $6 \pm 341i$ par un simple calcul on trouve,

pour $\alpha = 1 \pm 10i$, on trouve $u_5 = \dfrac{(1-10i)^5 - (1+10i)^5}{-20i} = 9005 = 5 \times 1801$,

pour $\alpha = 6 \pm 19i$, on trouve $u_5 = \dfrac{(6+19i)^5 - (6-19i)^5}{38i} = 6841$,

pour $\alpha = 6 \pm 341i$, on trouve $u_5 = \dfrac{(6+341i)^5 - (6-341i)^5}{682i} = 13\,479\,416\,281 = 3259 \times 4136\,059$.

On voit que ces valeurs ne sont pas des puissances de 13. Donc il n'existe pas d'entier v, on conclut que l'équation(0.0.5) n'a pas de solutions.

Pour $p = 7, 13$ toujours par le tableau (2.2.2) du théoreme du diviseur primitif (2.2.3) il n'existe pas d'entiers u ou v, donc l'équation(0.0.5) n'a pas de solutions. Pour $p = 11$, Il n'existe pas de valeurs de α pour lesquels u_{11} n'a pas de diviseurs primitifs, donc l'équation(0.0.5) n'a pas de solutions.

Toujours d'aprés le tableau, $u_{13}, u_{17}, u_{19}, u_{23}$ et u_{29} ont un diviseur primitif, donc ne sont pas des puissances de 13. En conclusion, notre équation n'a pas de solutions entières pour tout $p \geq 5$.

Supposons maintenant que $13 \mid x$, donc $x = 13^a x'$avec $13 \nmid x'$. Par les mêmes arguments, on trouve $y = 13^b y'$ avec $13 \nmid y'$, alors (0.0.5) devient

$$13^{2a}x'^2 + 13^{2m} = 13^{nb}y'^n \tag{2.3.2}$$

On distingue trois cas:

i) $2a = \min(2a, 2m, nb)$ alors (2.3.2) devient

$$x'^2 + 13^{2m-2a} = 13^{nb-2a}y'^n$$

et considérons cette équation modulo 13, donc $nb - 2a = 0$, alors on aura

$$x'^2 + 13^{2(m-a)} = y'^n$$

avec $(x', y') = 1$, donc l'équation n'a pas de solutions.

ii) $2m = \min(2a, 2m, nb)$, alors (2.3.2) devient

$$13^{2a-2m}x'^2 + 1 = 13^{nb-2m}y'^n$$

et considérons cette équation modulo 13, on obtient

$$(13^{a-m}x')^2 + 1 = y'^n$$

Par le théorème de Catalan (Lemme 2.3.2), cette équation n'a pas de solutions en entiers positifs.

iii) $nb = \min(2a, 2m, nb)$ alors (2.3.2) devient

$$13^{2a-nb}x'^2 + 13^{2m-nb} = y'^n$$

et considérons cette équation modulo 13, on aura soit $2a - nb = 0$ ou $2m - nb = 0$

- Si $2a - nb = 0$, alors on aura $x'^2 + 13^{2m-nb} = y'^n$, nb est pair, alors cette équation n'a pas de solutions car l'exposant de 13 est pair.

-Si $2m - nb = 0$, alors on a $13^{2a-nb}x'^2 + 1 = y'^n$, nb est pair, alors cette équation devient $13^{2a-2m}x'^2 + 1 = y'^n$, donc par le théorème de Catalan cette équation n'a pas de solutions en entiers positifs. ■

2.3.3 Résolution de l'équation Diophantienne $x^2+13^{2m+1}=y^n$, $n\geq 3$.

La troisième equation qu'on a résolu est la suivante

Théorème 2.3.3 *Soit m un entier positif, l'équation Diophantienne (0.0.6) où $n\geq 3$ a excactement une famille de solutions donnée par*

$$(x,y,m,n)=(70\cdot 13^{3k},17\cdot 13^{2k},3k,3).$$

Preuve. Soit $k=2m+1$,ou $m>0$. si x est impair alors y est pair et on obtient $x^2+13^{2m+1}\equiv 6 \bmod(8)$ mais $y^n\equiv 0(\mathrm{mod}\, 8)$

ce qui est imposible donc on prend x pair et y impair.

Cas 1 : n impair.

- Pour $n\geq 5$, et n est n'st pas un multiple de 3. Puisque le nombre de classes de $\mathbb{Q}(\sqrt{-13})$ est 2, l'équation (0.0.6) n'a pas de solutions en entiers strictement positifs [1].

- Il nous reste à considérer l'équation pour $n=3$.

Supposons que $13\mid x$, alors $13\mid y$, donc on pose $x=13^a.X$ et $y=13^b.Y$ avec $p\gcd(13,X)=p\gcd(13,Y)=1$. L'équation (0.0.6) devient :

$$13^{2a}X^2+13^{2m+1}=13^{3b}.Y^3$$

où $3b=\min(2a,2m+1,3b)$, l'équation devient

$$13^{2a-3b}X^2+13^{2m-3b+1}=Y^3$$

Considérons cette équation modulo 13, on obtient $2a=3b$, alors

$$X^2+13^{2m'+1}=Y^3 \tag{2.3.3}$$

avec $m'=m-a$.

Résolution de (2.3.3) :

Nous factorisons l'équation (2.3.3) dans $\mathbb{Z}\left[\sqrt{-13}\right]$, on aura

$$(X+13^{m'}\sqrt{-13}).(X-13^{m'}\sqrt{-13})=Y^3$$

Or, en termes d'idéaux, on obtient

$$\langle Y\rangle^3 = \left\langle X + 13^{m'}\sqrt{-13}\right\rangle . \left\langle X - 13^{m'}\sqrt{-13}\right\rangle .$$

Mais les idéaux $\left\langle X + 13^{m'}\sqrt{-13}\right\rangle , \left\langle X - 13^{m'}\sqrt{-13}\right\rangle$ sont premiers entre eux dans $\mathbb{Z}\left[\sqrt{-13}\right]$. En effet, soit P un idéal premier divisant à la fois $\left\langle X + 13^{m'}\sqrt{-13}\right\rangle$ et $\left\langle X - 13^{m'}\sqrt{-13}\right\rangle$, alors $\left\langle X + 13^{m'}\sqrt{-13}\right\rangle \in P, \left\langle X - 13^{m'}\sqrt{-13}\right\rangle \in P$, $2X \in P$, donc $P \mid \langle 2X\rangle$, et $P \mid \langle Y\rangle$, car il intervient dans la décomposition de $\langle Y\rangle^3$ en produit d'idéaux premiers. Passant aux normes, il vient $N(P) \mid N(2X) = 4X^2$, $N(P) \mid N(Y) = Y^2$. Puisque Y est impair, $N(P)$ est impair, d'où $N(P) \mid X^2$ et $N(P) \mid Y^2$, or $\langle P\rangle \neq \langle 1\rangle$, donc $N(P) \neq 1$, et X, Y ont un diviseur commun différent de 1, contradiction le fait que X et Y sont premiers entre eux. Alors chacun d'eux est le cube d'un idéal dans $\mathbb{Z}\left[\sqrt{-13}\right]$, alors

$$\left\langle X + 13^{m'}\sqrt{-13}\right\rangle = \mathfrak{a}^3,$$

pour un certain idéal $\mathfrak{a}$.

Puisque le nombre de classes de $\mathbb{Z}\left[\sqrt{-13}\right]$ égal 2 est premier avec 3, alors $\mathfrak{a}$ est principal (Lemme 1.3.2) donc

$$\mathfrak{a} = \langle j\rangle ,$$

alors

$$\left\langle X + 13^{m'}\sqrt{-13}\right\rangle = \langle j\rangle^3 ,$$

où $\gamma = \pm j \in \mathbb{Z}\left[\sqrt{-13}\right]$ (Les unités de $\mathbb{Z}\left[\sqrt{-13}\right]$ sont ± 1). Soit

$$\gamma = u + v\sqrt{-13}, u, v \in \mathbb{Z},$$

alors on obtient

$$X + 13^{m'}\sqrt{-13} = \pm(u + v\sqrt{-13})^3 \quad \text{et} \quad Y = u^2 + 13v^2 \quad ,$$

En identifiant les parties réelles et imaginaires, on trouve :

$$\pm X = 39uv^2 - u^3,$$

et

$$13^{m'} = 13v^3 - 3u^2v, \tag{2.3.4}$$

utilisant l'équation (2.3.4), on trouve

$$\begin{aligned} 13^{m'} &= 13v^3 - 3u^2v \\ &\Longleftrightarrow\ 13^{m'} = v(13v^2 - 3u^2) \\ &\Longleftrightarrow\ \begin{cases} v = 13^{\alpha} \\ 13v^2 - 3u^2 = 13^{\beta}, \end{cases} \alpha + \beta = m'. \end{aligned}$$

alors,

$$3u^2 = 13^{2\alpha+1} - 13^{\beta},$$

avec $2\alpha + 1 \geq \beta$, donc

$$3u^2 = 13^{\beta}(13^{2\alpha-\beta+1} - 1),$$

mais $p\gcd(3, 13) = 1$, alors $u^2 = 13^{\beta}.d$ où β est pair est d est un carré parfait.

Remplaçons les valeurs de u et v dans (0.0.6), on trouve

$$(9.13^{2\alpha+2\beta+1}).d^2 - (6.13^{4\alpha+\beta+2}).d + (13^{6\alpha+3} - 13^{2\alpha+2\beta+1}) = 0,$$

qui est une équation du deuxième degré de discriminant $\Delta = 36.13^{4\alpha+4\beta+2}$ et solutions

$$\begin{cases} d_1 = \dfrac{13^{2\alpha-\beta+1} - 1}{3} \in \mathbb{N} \\ d_2 = \dfrac{13^{2\alpha-\beta+1} + 1}{3} \notin \mathbb{N} \end{cases},$$

donc $d = \dfrac{13^{2\alpha-\beta+1} - 1}{3}$, mais d est un carré parfait alors,

$$d = s^2 \Longleftrightarrow 3s^2 + 1 = 13^{2\alpha-\beta+1},$$

qui a une seule solution (Théorème 2.3.1),

$$\begin{cases} s = 2 \\ \beta = 2\alpha \end{cases},$$

ainsi, $d = 4$ et $\beta = 2\alpha$, on trouve $u^2 = 4.13^{2\alpha}$ donc $u = \pm 2.13^{\alpha} \Rightarrow u = \pm 2.v$.

Don on a

$$m' = 3\alpha,\ X = 70.13^{3\alpha},\ Y = 17.13^{2\alpha}.$$

mais $13 \nmid X$ et $13 \nmid Y$, alors

$$X = 70, Y = 17, \quad \alpha = \beta = m' = 0,$$

et on a $3b = 2a$ implique $a = 3k$, $b = 2k$, $k > 0$, $m = a = 3k$. Donc toutes les solutions de (0.0.6) où $n = 3$ sont données par :

$$x = 70.13^{3k},\ y = 17.13^{k},\ m = 3k$$

** $2a = \min(2a, 2m + 1, 3b)$, alors on obtient

$$X^2 + 13^{2m-2a+1} = 13^{3b-2a}.Y^3$$

Considérons cette équation modulo 13, on obtient $3b = 2a$,alors

$$X^2 + 13^{2m'+1} = Y^3$$

avec $m' = m - a$ et $m \geq a$. Et cette dernière est exactement (2.3.3).

**$2m + 1 = \min(2a, 2m + 1, 3b)$, alors on obtient

$$13^{2a-2m-1}X^2 + 1 = 13^{3b-2m-1}.Y^3$$

Considérons cette équation modulo 13, on obtient soit $2a-2m = 1$, ce qui est impossible ou $3b - 2m = 1$ alors

$$13^{2a-2m-1}X^2 + 1 = Y^3$$

qui est impossible (Lemme 2.3.1).

- Pour $n > 3$, et n est un multiple de 3, on obtient :

$x^2 + 13^{2m+1} = y^{3n'}$, avec $n' > 1$, ceci implique que $x^2 + 13^{2m+1} = (y^{n'})^3$, avec solution $(x, y^{n'}) = (70.13^{3\alpha}, 17.13^{2\alpha})$, alors $y^{n'} = 17.13^{2\alpha}$ qui est impossible alors $n' > 1$.

-Cas 2 : n est pair, alors il est suffisant de prendre le cas $n = 4$, donc l'équation (0.0.6) devient :

$$(y^2 + x).(y^2 - x) = 13^{2m+1}$$

Nous distinguons deux cas :

1- $p\gcd(x, y) = 1$, on aura :

$$\begin{cases} y^2 + x = 13^{2m+1} \\ y^2 - x = 1 \end{cases}$$

ainsi

$$2y^2 + 1 = 13^{2m+1}$$

ce qui est impossible modulo 13.

2- Supposons que $13 \mid x$, alors $x = 13^a X$ avec $p\gcd(X, 13) = 1$ et $a \geq 1$ et ceci implique que $y = 13^b.Y$, où $p\gcd(Y, 13) = 1$ et $b \geq 1$, donc on conclut que $p\gcd(X, Y) = 1$. Alors l'équation (0.0.6) devient

$$13^{2a}X^2 + 13^{2m+1} = 13^{4b}Y^4$$

i) Si $2a = \min(2a, 2m + 1, 4b)$, on aura

$$X^2 + 13^{2m-2a+1} = 13^{4b-2a}Y^4$$

Considerons cette équation modulo 13, on obtient $4b - 2a = 0$, donc

$$X^2 + 13^{2m-2a+1} = Y^4$$

ce qui est impossible. ($2^{\text{ième}}$ cas avec $p\gcd(X, Y) = 1$).

ii) Si $2m + 1 = \min(2a, 2m + 1, 4b)$, on obtient

$$13^{2a-2m-1}X^2 + 1 = 13^{4b-2m-1}Y^4$$

Considerons cette équation modulo 13, on aura $4b - 2m - 1 = 0$ ce qui est impossible.

iii) Si $4b = \min(2a, 2m + 1, 4b)$, on abtient

$$13^{2a-4b}X^2 + 13^{2m+1-4b} = Y^4$$

Considérons cette équation modulo 13, on aura soit $2a - 4b = 0$ ou $2m + 1 - 4b = 0$. Si $2a - 4b = 0$, on obtient $X^2 + 13^{2m+1-4b} = Y^4$, ce qui est impossible, et le second cas est évidemment impossible. ■

Chapitre 3

Equation Diophantienne en Nombres Triangulaires

3.1 Introduction

Habituellement, on parle des nombres paires, impaires et premiers, mais il y'a bien d'autres jolis nombres, comme les nombres de Fibonacci, les nombres amis, les nombres parfaits, ...etc.

D'autres nombres sont particulièrement élégants quand ils dénombrent les points qui forment une figure géométriques.

Un nombre triangulaire est un nombre de la forme $T_n = \sum_{k=0}^{n} k = n(n+1)/2$, où n est un entier naturel, donc les premiers nombres triangulaires sont $0, 1, 3, 6, 10, 15, 21, 28$,... (*sequence A000217)* en [40]. Un résultat très connu sur les nombres triangulaires est que X est un nombre triangulaire si et seulement si $8X + 1$ est un carré parfait. Ces nombres peuvent être considérés comme les nombres de points nécessaires pour construire un triangle.

Beaucoup d'auteurs s'intéressent aux équations Diophantiennes liées aux nombres triangulaires. par exemple, *W. Sierpinski* [38], [39] a démontré que dans la série de nombres triangulaires il y'a une infinités qui sont des carrés c'est à dire, il a résolu l'équation

$$T_x = y^2,\ x, y \in \mathbb{N}.$$

Il a affirmé que si $T_x = y^2$ alors le plus petit nombre triangulaire carré qui est plus grand que T_x est $T_{3x+4y+1}$. Par exemple si on prend $T_1 = 1 = 1^2$ alors $T_8 = 36 = 6^2$, donc il a construit une suite de nombres triangulaires carrés.

Dans ce chapitre, on va donner une méthode de résolution de l'équation Diophantienne (0.0.4) [19].

Les articles [5], [17], [22], [36], [37] donnent plusieurs résultats interessants de la résolubilité des équations Diophantiennes liées aux nombres triangulaires. Le but de ce chapitre est binaire : dans un premier lieu, nous donnons toutes les solutions de l'équation (0.0.4), puis, nous donnons une méthode de trouver explicitement (et rapidement) des familles infinies de solutions de l'équation (0.0.4) dans lequel de nombreuse nouvelles suites entières sont derivées.

Ce genre d'équation a été résolu pour la première fois par Sièrpiski [37]. Il a donné une démonstration de la proposition suivante

Proposition 3.1.1 *Il existe une infinité de paires de nombres triangulaires dont la somme ainsi que la différence sont des nombres triangulaires*

Il a démontré aussi dans son article [38], qu'il existe une infinité de nombres naturels x et y vérifiant les deux équations

$$t_x + t_{2y} = t_{3y} \quad \text{et} \quad t_x - t_{2y} = t_{y-1}, \tag{3.1.1}$$

La résolution de l'équation (3.1.1) nous ramène à démontrer que l'équation

$$x^2 + x = 5y^2 + y,$$

admet une infinité des solutions (x, y).

Notre méthode de résolution est totalement différente à celle de Sieprinki. Nous avons utlisé la théorie des matrices en réduisant notre équation aux système d'équations.

3.2 Quelques identités sur les nombres triangulaires

Dans cette section, nous donnons quelques propriétés des nombres triangulaires et quelques résultats liés aux équations Diophantiennes en nombres triangulaires. Commençons par :

Proposition 3.2.1 *Soit T_n le nombre triangulaire de rang $n \geq 0$, alors on a*

1) $T_{n-1} + T_n = n^2$,

2) $T_n^2 - T_{n-1}^2 = n^3$,

3) $T_n^2 + T_{n-1}^2 = T_{n^2}$,

4) $T_{2n} = 3T_n + T_{n-1}$,

5) $T_{2n} - 2T_n = n^2$,

6) $8T_n + 1 = (2n+1)^2$.

Une résolution de l'équation (3.1.1)

Dans l'introduction de ce chapitre nous avons donné un résultat lié à l'équation Diophantienne (3.1.1). Nous proposons une démonstration.

Comme le système

$$\begin{cases} T_x + T_{2y} = T_{3y} \\ T_x - T_{2y} = T_{y-1} \end{cases}, \tag{3.2.1}$$

est équivalent à

$$\begin{aligned} x^2 + x &= 5y^2 + y, \\ x^2 + x &= y^2 + y + 4y^2, \end{aligned}$$

Cela implique

$$(x + \frac{1}{2})^2 - \frac{1}{4} = (y + \frac{1}{2})^2 - \frac{1}{4} + 4y^2,$$

Multiplions les deux cotés par 4, on obtient

$$(2x+1)^2 - 1 = (2y+1)^2 - 1 + 16y^2$$

qui est équivalent à

$$A^2 = B^2 + C^2, \tag{3.2.2}$$

avec $A = 2x+1$, $B = 2y+1$ et $C = 4y$.

Soit d un diviseur commun de B et C, donc $d \mid 2y+1$ et $d \mid 4y$ alors $d \mid 2$. Si $d = 2$, donc B et C sont pairs ce qui implique que A est pair : contradiction du fait que $A = 2x+1$, donc B et C sont premiers entre eux. Par conséquent le triplet (A, B, C) est un triplet pythagoricien, alors

$$(A, B, C) = (a^2 + b^2, a^2 - b^2, 2ab),$$

pour certains entiers a et b premiers entre eux. Donc

$$a^2 - b^2 - ab = 1,$$

Comme A est impair, donc a et b sont de différente parité. Soit a impair et b pair, alors on a

$$\begin{aligned}(a - \frac{b}{2})^2 - \frac{5}{4}b^2 &= 1,\\ (2a - b)^2 - 5b^2 &= 4.\end{aligned}$$

Posons $R = 2a - b$, $S = b$, la dernière équation devient

$$R^2 - 5S^2 = 4. \tag{3.2.3}$$

C'est une équation de Pell qui a une infinité de solutions. Par conséquent il existe une infinité de paires (x, y) qui satisfont le système (3.2.1).

Mais d'après [24] , (corollaire 14), toutes les solutions de (3.2.3) sont données par

$$(R, S) = (L_{2n}, F_{2n}), \qquad n \geq 1,$$

où $(F_n)_{n\geq 0}$ et $(L_n)_{n\geq 0}$ sont les suites de *Fibonacci* et de *Lucas* respectivement. Alors

$$(a, b) = (\frac{F_{2n} + L_{2n}}{2}, F_{2n}),$$

Comme b est pair par hypothèse, alors $F_{2n} \equiv 0 (\mathrm{mod}\, 2)$ or $F_{2n} = F_n.L_n$ pour tout $n \geq 0$, alors $F_n \equiv 0 (\mathrm{mod}\, 2)$ ou $L_n \equiv 0 (\mathrm{mod}\, 2)$ ce qui implique que $n \equiv 0 (\mathrm{mod}\, 3)$, donc $n = 3k$ pour un certain entier $k \geq 1$.

Par un simple calcul, on trouve

$$y_k = \frac{F_{6k}^2 + F_{12k}}{4}, \quad k \geq 1$$

et

$$x_k = \frac{5F_{6k}^2 + L_{6k}^2 + 2F_{12k} - 4}{8} \quad k \geq 1.$$

Il est bien connu que l'équation $T_x = y^2$ est équivalente à une équation de Pell de la forme

$$U^2 - 8y^2 = 1, \tag{3.2.4}$$

où $U = 2x + 1$. La solution fondamentale de léquation de Pell (3.2.4) est $(U, y) = (3, 1)$ et pour tout $n \geq 0$, on a

$$U_n = \frac{1}{2}\left[(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n\right],$$

et

$$y_n = \frac{1}{4\sqrt{2}}\left[(3 + 2\sqrt{2})^n - (3 - 2\sqrt{2})^n\right].$$

Et comme $U_n = 2x_n + 1$ pour tout $n \geq 0$, alors on aura

$$x_n = \left[\frac{(1 + \sqrt{2})^n + (1 - \sqrt{2})^n}{2}\right]^2, \qquad n \geq 0,$$

ce qui prouve qu'il y'a une infinité de nombres triangulaires carrés.

Remarque 3.2.1 *Pour tout nombre impair x qui satisfait $t_x = y^2$ alors x est aussi un carré.*

En effet, réécrivons la formule de U_n comme suit

$$2x_n + 1 = \frac{1}{2}\left[(3 + 2\sqrt{2})^n + (3 - 2\sqrt{2})^n\right],$$

donc

$$x_n = \frac{1}{4}\left[(1 + \sqrt{2})^{2n} + (1 - \sqrt{2})^{2n} - 2\right],$$

alors

$$x_n = \frac{1}{4}\left[(1 + \sqrt{2})^{2n} + (1 - \sqrt{2})^{2n} + 2((1 + \sqrt{2})^n.(1 - \sqrt{2})^n)\right],$$

donc

$$x_n = \frac{1}{4}\left[(1 + \sqrt{2})^n + (1 - \sqrt{2})^n\right]^2.$$

qui est un carré.

3.3 Résolution de l'équation $T_X + T_Y = T_Z$.

Dans cette section, nous proposons une méthode technique et calculatoire pour déterminer toutes les solutions de l'équation (0.0.4). Nous donnerons d'abord une factorisation de l'équation (0.0.4) en utlisant un résultat connu, puis nous démontrons qu'il existe des matrices carées M d'ordre 3 dans l'espace $\{1, 2, 3\}^9$ telles que si (x, y, z) est une solution de (0.0.4) alors $M \times (x, y, z)$ l'est aussi. Nous construisons ensuite des nouvelles suites en multipliant une solution donnée récurcivement par la matrice M.

3.3.1 Solution générale

Commençons par quelques résultas importants et techniques .

Lemme 3.3.1 *Soit $a, b, c, d \in N$. alors $ab = cd$ si et seulement si il existe $p, q, m, n \in N$ tels que $a = mn,\ b = pq,\ c = mp$ and $d = nq$.*

Preuve. Soit $a = \prod_{i \in A \subset \mathbb{N}} p_i^{\alpha_i}$ et $b = \prod_{i \in B \subset \mathbb{N}} q_i^{\beta_i}$ ou p_i, q_i sont premiers, $\alpha_i, \beta_i \in N$ et A, B sont des ensembles finis. Le fait que

$$cd = \prod_{i \in A \subset \mathbb{N}} p_i^{\alpha_i} \prod_{i \in B \subset \mathbb{N}} q_i^{\beta_i}$$

implique que

$$c = \prod_{i \in A' \subset A} p_i^{\alpha'_i} \prod_{i \in B' \subset B} q_i^{\beta'_i} \ etd = \prod_{i \in A'' \subset A} p_i^{\alpha''_i} \prod_{i \in B'' \subset B} q_i^{\beta''_i},$$

où $0 \leq \alpha'_i, \alpha''_i \leq \alpha_i,\ 0 \leq \beta'_i, \beta''_i \leq \beta_i$ avec $\alpha_i = \alpha'_i + \alpha''_i$ et $\beta_i = \beta'_i + \beta''_i$.

Si on pose

$$m = \prod_{i \in A' \subset A} p_i^{\alpha'_i},\ p = \prod_{i \in B' \subset B} q_i^{\beta'_i},\ n = \prod_{i \in A'' \subset A} p_i^{\alpha''_i} \ etq = \prod_{i \in B'' \subset B} q_i^{\beta''_i}$$

alors on obtient,

$$a = mn,\ b = pq,\ c = mp \text{ et } d = nq.$$

■

Lemme 3.3.2 *L'équation (0.0.4) est équivalente à $X(X+1) = (Z-Y)(Z+Y+1)$.*

Preuve. Remplaçons T_X par $\frac{X(X+1)}{2}$, T_Y par $\frac{Y(Y+1)}{2}$ et T_Z par $\frac{Z(Z+1)}{2}$ l'équation (0.0.4) devient

$$\frac{X(X+1)}{2} + \frac{Y(Y+1)}{2} = \frac{Z(Z+1)}{2}.$$

i.e.

$$X^2 + X + Y^2 + Y = Z^2 + Z. \tag{3.3.1}$$

alors

$$X^2 + X = Z^2 - Y^2 + Z - Y.$$

finalement

$$X(X+1) = (Z-Y)(Z+Y+1).$$

■

Maintenant, nous pouvons établir le théorème suivant

Théorème 3.3.1 *toutes les solutions entières de l'équation $T_X + T_Y = T_Z$ sont données par*

$$\begin{cases} X = mn \\ Y = \frac{1}{2}(nq - mp - 1) \\ Z = \frac{1}{2}(nq + mp - 1) \end{cases} : \ m, n, p, q \in \mathbb{N}$$

où $pq - mn = 1$ et $nq - mp - 1 \in 2N$.

Preuve. D'aprés le Lemme (3.3.2), l'équation (0.0.4) est équivalente à

$$X(X+1) = (Z-Y)(Z+Y+1),$$

alors, d'aprés le lemme (3.3.1), on a

$$\begin{cases} X = mn \\ X + 1 = pq \\ Z - Y = mp \\ Z + Y + 1 = nq \end{cases} : \ m, n, p, q \in N$$

Ainsi, on obtient

$$\begin{cases} X = mn \\ Y = \frac{1}{2}(nq - mp - 1) \\ Z = \frac{1}{2}(nq + mp - 1) \end{cases} : \ m, n, p, q \in \mathbb{N}$$

tels que $pq - mn = 1$ et $nq - mp - 1 \in (2\mathbb{N})$. ■

Remarque 3.3.1 *On peut établir l'identité suivante. Pour tout* $(n, m, p, q) \in (\mathbb{N})^4$, *on a*

$$T_{mn} + T_{\frac{nq-mp-1}{2}} = T_{\frac{nq+mp-1}{2}},$$

avec $pq - mn = 1$ *et* $nq - mp - 1 \in (2\mathbb{N})$.

En effet,

$$\begin{aligned}
T_{mn} + T_{\frac{nq-mp-1}{2}} &= \frac{mn(mn+1)}{2} + \frac{(\frac{nq-mp-1}{2})(\frac{nq-mp+1}{2})}{2} \\
&= \frac{4mn(mn+1) + (nq-mp)^2 - 1}{2} \\
&= \frac{4(mn)^2 + 4mn + (nq)^2 + (mp)^2 - 2(mn)(pq) - 1}{2} \\
&= \frac{4(mn)^2 + 4mn - 4(mn)(pq) + (nq)^2 + (mp)^2 + 2(mn)(pq) - 1}{2} \\
&= \frac{4(mn)^2 + 4mn - 4(mn)(pq) + (nq+mp)^2 - 1}{2} \\
&= \frac{4mn(mn - pq + 1) + (nq+mp)^2 - 1}{2} \\
&= \frac{(nq+mp)^2 - 1}{2} \\
&= \frac{\left(\frac{(nq+mp-1)}{2}\right)\left(\frac{(nq+mp+1)}{2}\right)}{2} \\
&= T_{\frac{nq+mp-1}{2}}.
\end{aligned}$$

Exemple 3.3.1 $p = 4,\ q = 7,\ m = 3$ *et* $n = 9$. *Il est clair que* $X = 27,\ Y = 25$ *et* $Z = 37$, *et* $T_{27} = 378,\ T_{25} = 325,\quad T_{37} = 703$, *ainsi* $T_{27} + T_{25} = T_{37}$.

3.3.2 Familles de solutions

Premièrement, notons qu'il n'est pas facile de trouver des entiers naturels m, n, p, q tels que $pq - mn = 1$ et $nq - mp - 1 \in (2\mathbb{N})$.

L'utilisation des matrices nous aide à obtenir un large nombres de solutions de (0.0.4). Dans cette section, nous allons construire de nombreuses familles infinies de solutions de notre équation triangulaire.

Par completion en carrés dans l'équation (3.3.1), on obtient

$$(X + \frac{1}{2})^2 + (Y + \frac{1}{2})^2 = (Z + \frac{1}{2})^2 + \frac{1}{4}.$$

Multiplions les deux cotés par 4, on aura

$$(2X + 1)^2 + (2Y + 1)^2 = (2Z + 1)^2 + 1.$$

Posons, $x = 2X + 1,\ y = 2Y + 1$ et $z = 2Z + 1$, on trouve

$$x^2 + y^2 = 1 + z^2. \tag{3.3.2}$$

Puisque la preuve de la proposition suivante se voit facilement, nous omettons sa preuve.

Proposition 3.3.1 *Les deux familles* $\begin{pmatrix} 1 \\ a \\ a \end{pmatrix}, \begin{pmatrix} a \\ 1 \\ a \end{pmatrix}$ *sont des solutions de (3.3.2) pour tout entier a.*

Théorème 3.3.2 *Il existe une matrice carée M d'ordre 3, à éléments dans* $\{1, 2, 3\}^9$, *telle que si* $\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ *est une solution de (3.3.2) alors M* $\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ *est aussi une solution.*

Preuve. Soit $M = \begin{pmatrix} A & B & C \\ E & F & G \\ L & M & N \end{pmatrix}$ et soit $\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix}$ une solution de (3.3.2).

Il est clair que

$$\begin{pmatrix} A & B & C \\ E & F & G \\ L & M & N \end{pmatrix} \begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} Ax_0 + By_0 + Cz_0 \\ Fy_0 + Gz_0 + Ex_0 \\ Lx_0 + My_0 + Nz_0 \end{pmatrix}.$$

Maintenant, si le système suivant

$$\begin{cases} A^2 - L^2 + E^2 = 1 \quad ...(1_0) \\ B^2 + F^2 - M^2 = 1 \\ C^2 + G^2 - N^2 = -1 \\ AB - LM + EF = 0 \\ AC - LN + EG = 0 \\ BC - MN + FG = 0 \end{cases}, \qquad (S)$$

est vérifié, alors

$$(Ax_0 + By_0 + Cz_0)^2 + (Fy_0 + Gz_0 + Ex_0)^2 - (Lx_0 + My_0 + Nz_0)^2 = 1.$$

Il en découle que

$$\begin{pmatrix} Ax_0 + By_0 + Cz_0 \\ Fy_0 + Gz_0 + Ex_0 \\ Lx_0 + My_0 + Nz_0 \end{pmatrix},$$

est une solution de (3.3.2).

Nous allons explorer, en cinq étapes, toutes les solutions du système (S) dans l'espace $\{1, 2, 3\}^9$.

*** Cas 1**: $A = L = E = 1$. on trouve

$$\begin{cases} B^2 + F^2 - M^2 = 1 \quad ...(1_1) \\ C^2 + G^2 - N^2 = -1 \\ B + F = M \quad ...(3_1) \\ C + G = N \\ BC - MN + FG = 0. \end{cases}$$

D'après (3_1), on obtient $F = 1$ ou $B = 1$, alors (1_1) implique que $B = M$ ou $F = M$ alors $F = 0$ ou $B = 0$, ce qui est impossible.

*** Cas 2 :** $A = 1,\ L = E = 2$. On aura

$$\begin{cases} B^2 + F^2 - M^2 = 1 \\ C^2 + G^2 - N^2 = -1 \\ B - 2M + 2F = 0 \quad ...(3_2) \\ C - 2N + 2G = 0 \quad ...(4_2) \\ BC - MN + FG = 0. \end{cases}$$

Les équations (3_2) et (4_2) impliquent que B et C sont pairs. Alors d'après

$$\begin{cases} M^2 - F^2 = 3 & ...(1_2) \\ N^2 - G^2 = 5 & ...(2_2) \\ M - F = 1 \\ N - G = 1 \\ MN - FG = 4. \end{cases}$$

L'équation (1_2) donne $M = 2, F = 1$ et (2_2) donne $N = 3, G = 2$. Alors

$$M_1 = \begin{pmatrix} A & B & C \\ E & F & G \\ L & M & N \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}.$$

*** Cas 3 :** $A = 1, L = E = 3$.

$$\begin{cases} B^2 + F^2 - M^2 = 1 \\ C^2 + G^2 - N^2 = -1 \\ B - 3M + 3F = 0 & ...(3_3) \\ C - 3N + 3G = 0 & ...(4_3) \\ BC - MN + FG = 0. \end{cases}$$

L'équations (3_3) et (4_3) nous donnent $B = C = 3$. Alors

$$\begin{cases} F^2 - M^2 = -8 \\ G^2 - N^2 = -10 & ...(2_3) \\ -M + F = -1 \\ -N + G = -1 \\ -MN + FG = -9. \end{cases}$$

Il est facile de voir que l'équation (2_3) est impossible dans $\{1, 2, 3\}^2$

*** Cas 4 :** $A = 2$.

L'équation (1_0) dans (S) implique que $L = 2, E = 1$. Donc, on a

$$\begin{cases} B^2 + F^2 - M^2 = 1 \\ C^2 + G^2 - N^2 = -1 \\ 2B - 2M + F = 0 & ...(3_4) \\ 2C - 2N + G = 0 & ...(4_4) \\ BC - MN + FG = 0. \end{cases}$$

L'équations (3_4) et (4_4) nous donnent $F = G = 2$. Ainsi

$$\begin{cases} M^2 - B^2 = 3 \quad ...(1_4) \\ N^2 - C^2 = 5 \quad ....(2_4) \\ M - B = 1 \\ N - C = 1 \\ BC - MN + 4 = 0. \end{cases}$$

L'équation (1_4) nous donne $M = 2, B = 1$ et (2_4) donne $N = 3, C = 2$. On obtient

$$M_2 = \begin{pmatrix} A & B & C \\ E & F & G \\ L & M & N \end{pmatrix} = \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 3 \end{pmatrix}.$$

*** Cas 5 :** $A = 3$.

L'équation (1_0) dans (S) implique que : $L = 3, E = 1$. Maintenant

$$\begin{cases} B^2 + F^2 - M^2 = 1 \\ C^2 + G^2 - N^2 = -1 \\ 3B - 3M + F = 0 \quad ...(3_5) \\ 3C - 3N + G = 0 \quad ...(4_5) \\ BC - MN + FG = 0. \end{cases}$$

Les équations (3_5) et (4_5) nous donnent $F = G = 3$, ainsi

$$\begin{cases} M^2 - B^2 = 8 \\ N^2 - C^2 = 10 \quad ...(2_5) \\ B - M + 1 = 0 \\ C - N + 1 = 0 \\ BC - MN + 9 = 0. \end{cases}$$

Il est facile de voir que l' équation (2_5) est impossible dans $\{1, 2, 3\}^2$. ■

Corollaire 3.3.1 *L' équation (0.0.4) admet une infinité de solutions.*

Preuve. Let $M = M_1$ et $\begin{pmatrix} x_0 \\ y_0 \\ z_0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ une solution de (3.3.2) alors $M^n \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ est une solution de (3.3.2) pour tout entier $n \geq 0$. ■

3.3.3 Nouvelles suites

En utilisons "the on-line Encyclopedia" des suites numériques [40], nous pouvons facilement vérifier que les deux suivantes suites formées par les solutions X de l'équation triangulaire (0.0.4) :

$$1, 5, 35, 203, 1179, 6929, 40391, 235415, 1372105, 7997213...$$

et

$$0, 8, 54, 322, 1884, 10988, 64050, 373318, 2175864, 12681872, ...$$

sont nouvelles.

3.3.4 Constructions :

1 Nous commençons par $\begin{pmatrix} 3 \\ 1 \\ 3 \end{pmatrix}$ une solution de (3.3.2), d'aprés le théoreme 2, par multiplication récursive par M_1, on obtient

$$\begin{pmatrix} 11 \\ 13 \\ 17 \end{pmatrix}, \begin{pmatrix} 71 \\ 69 \\ 99 \end{pmatrix}, \begin{pmatrix} 407 \\ 409 \\ 577 \end{pmatrix}, \begin{pmatrix} 2379 \\ 2377 \\ 3363 \end{pmatrix}, \begin{pmatrix} 13\,859 \\ 13\,861 \\ 19\,601 \end{pmatrix}, \begin{pmatrix} 80\,783 \\ 80\,781 \\ 114\,243 \end{pmatrix}, \begin{pmatrix} 470\,831 \\ 470\,833 \\ 665\,857 \end{pmatrix},$$
$$\begin{pmatrix} 2744\,211 \\ 2744\,209 \\ 3880\,899 \end{pmatrix}, \begin{pmatrix} 15\,994\,427 \\ 15\,994\,429 \\ 22\,619\,537 \end{pmatrix}, ... \text{ sont aussi des solutions de(3.3.2).}$$

On obtient,

$$x = 3, 11, 71, 407, 2379, 13859, 80783, 470831, 2744211, 15\,994\,427, ...$$

Or $x = 2X + 1$, donc

$$X = 1, 5, 35, 203, 1179, 6929, 40391, 235415, 1372105, 7997213, ...$$

est une nouvelle suite d'entiers impairs formée par les solutions X de notre équations triangulaire (0.0.4).

2 Nous commençons par $\begin{pmatrix} 1 \\ 5 \\ 5 \end{pmatrix}$ une solution de (3.3.2), d'après le théorème 2, par multiplication récursive par M_2, on obtient

$$\begin{pmatrix} 17 \\ 21 \\ 27 \end{pmatrix}, \begin{pmatrix} 109 \\ 113 \\ 157 \end{pmatrix}, \begin{pmatrix} 645 \\ 649 \\ 915 \end{pmatrix}, \begin{pmatrix} 3769 \\ 3773 \\ 5333 \end{pmatrix}, \begin{pmatrix} 21\,977 \\ 21\,981 \\ 31\,083 \end{pmatrix}, \begin{pmatrix} 128\,101 \\ 128\,105 \\ 181\,165 \end{pmatrix}, \begin{pmatrix} 746\,637 \\ 746\,641 \\ 1055\,907 \end{pmatrix},$$
$$\begin{pmatrix} 4351\,729 \\ 4351\,733 \\ 6154\,277 \end{pmatrix}, \begin{pmatrix} 25\,363\,745 \\ 25\,363\,749 \\ 35\,869\,755 \end{pmatrix}, \ldots \text{ sont aussi des solutions de (3.3.2).}$$

On obtient

$$x = 1, 17, 109, 645, 3769, 21977, 128101, 746637, 4351729, 25\,363\,745, \ldots$$

Mais $x = 2X + 1$, alors

$$X = 0, 8, 54, 322, 1884, 10988, 64050, 373318, 2175864, 12681872, \ldots$$

est une nouvelle suite d'entiers pairs formée par les solutions de notre équation triangulaire (0.0.4).

Conclusion et perspectives

Les différentes méthodes de résolution exposées le long de cette Thèse nécessitent la maitrise d'outils algébriques sophistiqués.

Dans un premier lieu, on a résolu complètement l'équation Diophantienne $x^2 + 13^p = y^n$ en utlisant la moderne théorie algébrique des nombres et la récente théorie des diviseurs primitifs.

Dans un second lieu, on a résolu complètement l'équation Diophantienne en nombres traingulaires $T_X + T_Y = T_Z$ en utilisant une méthode imaginative basée sur les techniques classiques de résolution (factorisation, paramétrisation, identités, matrices,...).

Mes perspectives sont d'étudier les techniques de résolution des formes modulaires et des formes linéaires du logarithme, dans le but de résoudre les équations Diophantiennes $x^2 - c = y^n$, $x^n - y^m = c$, $x^3 + c = y^n$ et bien d'autres.

Bibliographie

[1] S.A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + q^{2k+1} = y^n$, J. Number Theory, 95 (2002), 95–100.

[2] S.A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + 2^k = y^n$, Internat. J. Math. and Math. Sci.. Vol. 20, 2 (1997), 299 – 304.

[3] S.A. Arif and F. S. Abu Muriefah, On the Diophantine equation $x^2 + 5^{2k+1} = y^n$, The Arabian J. for Sci. and Engineering, 26(1A), 53–62, 2001.

[4] Abu Muriefah, F. S., Arif, S. A., The Diophantine equation $x^2 + 3^m = y^n$, Int. J. Math. Math. Sci. 21, no. 3, 619–620, (1998).

[5] Michael A. Bennett, . A question of Sierpinski on triangular numbers, Integers 5 (2005), no. 1, A25, 2 pp.

[6] M. A. Bennett and C. M. Skinner. Ternary Diophantine equations via Galois representations and Modular Forms. Canad. J. math. 56:23–54, 2004.

[7] Y.F. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math., 539, 75–122, 2001.

[8] Yu. Bilu, G. Hanrot and P. M. Voutier. Existence of Primitive Divisors of Lucas and Lehmer Numbers. With an appendix by M. Mignotte, J. Reine Angew. Math. 539 (2001): 75–122.

[9] Y. Bugeaud, F. Luca, M. Mignotte, S. Siksek, Almost Powers in the Lucas Sequence. Journal de Théorie des Nombres de Bordeaux. 20 (2008), no 3, 555–600.

[10] R. D. Carmechael, On the Numerical Factorsof Certain Arithmetic Forms, The Americain Mathematical Monthly, Vol,. 16, No. 10, (Oct 1909).

[11] H.Cohen, Explicit Methods for Solving Diophantine Equations. Tucson, Arizona Winter School, 2006.

[12] Henri. Cohen, Number Theory, Vol 1, Tools and Diophantine equations, GTM 239 Springer, new York, 2007.

[13] J.H.E. Cohn, The Diophantine equation $x^2 + C = y^n$, Acta Arith. 65 (1993), No.4, 367–381.

[14] J. H. E. Cohn, The Diophantine equation $x^2 + 2^k = y^n$, Arch. Math (Basel) 59, no. 4, 341–344, (1992).

[15] J.H.E, COHN. The diophantine equation $x^2 + 3 = y^n$, Glasgo Math. J., 35 (1993), 203-206.

[16] J.H.E. Cohn, The Diophantine equation $x^2 + C = y^n$, Acta Arith., 65(4), 367–381, 1995.

[17] John A. Ewell, On sums of three triangular numbers. Fibonacci Quart. 26 (1988), no. 4, 332–335. Computer Science 5011 (2008), 430–442.

[18] A. Hamtat, D. Behloul, On the Diophantine equation $x^2 + 13^k = y^n$. Journal of the Indian Mathematical Society, V 84 (3-4), 2017, 191-200.

[19] A. Hamtat, D. Behloul, On a Diophantine Equation on Triangular Numbers, Miskolc Mathematical Notes. 18, no. 2, 779-186.

[20] Z, Hui. Lin, Mao Hua Lec, On some generalized Lebesgue–Nagell equations. Journal of Number Theory 131 (2011) 458–469.

[21] Kenneth. Ireland, Micheal. Rosen, A classical Introduction to Modern Number Theory, Second Edition, Springer, New York 1990.

[22] Ide, Joshua; Jones, Lenny. Arithmetic progressions involving triangular numbers and squares. J. Comb. Number Theory 5 (2013), no. 3, 165–179.

[23] R. Keskin, Karaatli. Olcay. Some new properties of balancing numbers and square triangular numbers. J. Integer Seq. 15 (2012), no. 1, Article 12.1.4, 13 pp.

[24] R. Keskin, M. Güney. Positive integer solutionsof the Pell equation $x^2 - dy^2 = N$, $d \in \{k^2 \pm 4, k^2 \pm 1\}$ and $N \in \{\pm 1, \pm 4\}$. arXiv:1304.6887v1.[math.NT], April 2013.

[25] J.L. Lesage, Différece entre puissances et carrés d'entiers, J. Number Theory, 73 (1998), 390-425.

[26] V. A. Lebesque, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, Nouvelle Annales des Mathématiques 9(1), 178–181 (1850).

[27] F. Luca, On the Diophantne Equation $x^2 + 2^a 3^b = y^n$, Int. J. Math. Math. Sci. 29.4 (2002) 239–244

[28] F. Luca, Effective methods for Diophantine equations, Universidad Nacional Autonoma de Mexico (2009).

[29] F. Luca. On the equation $x^2 + 2^a 3^b = y^n$. Int. J. Math. Math. Sci. 29 (2002), no. 4, 239-244.

[30] F. Luca , A. Togbé. On the Diophantine equation $x^2 + 2^a 5^b = yn$. Int. J. Number Theory 4 (2008), no. 6, 973-979.

[31] M. Mignotte, B.M.M de Weger, On the equations $x^2 + 74 = y^5$and $x^2 + 86 = y^5$. Glasgow Math. J. 38/1 (1996) 77{85.

[32] T. Nagell, The diophantine equation $x^2 + 7 = 2^n$, Nordisk. Mat. Tidsker, 30, 62-64, Ark.Mat., 4 (1960), 185-187.

[33] T.Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknown, Nova Acta Reg. Soc. Upsal.Ser. 4 (1955), no.16, 1–38.

[34] S. Siksek, J.E. Cremona, On the Diophantine equation $x^2 + 7 = y^m$, Acta Arith. 109 (2) (2003) 143–149.

[35] Pierre. Samuel, Théorie algébriques des nombres, Hermann, Paris.1967.

[36] W. Sierpinski, Sur trois nombres triangulaires en progression arithmétique a différence triangulaire, Elem. Math. 20 (1965), 79-81.

[37] W. Sierpinski, A. Schinzel, Sur les triangle rectangulaires dont les deux cotes sont des nombres triangulaires, Buul.Soc.Math.Phys.Serbie 13 (1961), 145-147.

[38] W. Sierpinski, Triangular numbers, Biblioteczka Matematyczna 12, Warszawa. 1962.

[39] W. Sierpinski, Theorem on triangular numbers, Elem. Math. 23 (1968), 31-32.

[40] N.J.A Sloane, The On-Line Encyclopedia of Integer Sequences : https://oeis.org.

[41] L. Tao, On the Diophantine equation $x^2 + 5^m = y^n$, Ramanujan J. 19 (2009) 325–338.

[42] A. Thue, Uber die Unlösbarkeit der Gleichung $ax^2 + bx + c = dy^n$ in grossen ganzen Zahlen x and y. Arch. Math. og Naturvidenskab, Kristiania, Bd XXXIV (1916), 1–6.

[43] L. Maohua, A note on the Diophnatine equation $x^2 + 7 = y^n$, Glascow Mathematical journal,V 39, 1997, 59-63.