N° d'ordre : 91/2019-C/MT

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université des Sciences et de la Technologie Houari Boumediene
Faculté de Mathématiques

THÈSE de Doctorat

EN VUE DE L'OBTENTION DU GRADE DE DOCTEUR

En Mathématiques
Spécialité : Arithmétique Codage et Combinatoire

Présentée par
BERBARA NACIRA
Thème

Nombre de Solutions d'Équations Diophantiennes

Soutenue publiquement le 16/11/2019, devant le Jury composé de :

Mr BENCHERIF Farid	Professeur	à l'USTHB	Président
Mr KIHEL Omar	Professeur	à l'Univ. Brock,	Directeur
Mr BENSEBA Boualem	Maitre de conférence/A	à l'Univ. USTHB	Co-Directeur
Mr BERRACHDI Abdelhafid	**Professeur**	à l' Univ. USTHB	Examinateur
Mr BELGAHABA Kacem.	**Professeur**	à l'Univ. Ahmed Benbella1	Examinateur
Mr DJEBBAR Bachir	**Professeur**	à l'Univ. USTO M.B	Examinateur
Mr AIBOUDI Mohammed	Maitre de conférence/A	à l'Univ. Ahmed Benbella1	Invité

Table des matières

Introduction

Notre sujet porte sur l'étude et la résolution des équations diophantiennes. où nous nous intéressons au problème de la détermination du nombre de solutions d'une équation diophantienne et pour lequel nous tenterons d'améliorer certains résultats récents. On appelle équation diophantienne, une équation polynomiale à une ou plusieurs inconnues de la forme

$$f(x, y, z, \ldots\ldots) = 0 \qquad (1)$$

dont les solutions sont recherchées parmi les entiers rationnels.

L'intérêt que porte beaucoup de mathématiciens aux équations diophantienne vient de leurs utilisations dans de multiples domaines des mathématiques pures et appliquées tels que la théorie des nombres, l'analyse diophantienne et en cryptographie.

L'étude des équations diophantienne fait appel à plusieurs notions d'arithmétique, d'algèbre, d'analyse et de théorie des nombres. Une connaissance très approfondie de la notion de fractions continues est indispensable notamment dans l'étude d'un type d'équations diophantiennes de la forme $x^2 - dy^2 = N$ pour N dans $\mathbb{Z}$, dites de Pell généralisées.

La principale question qui a été posé au début était la suivante : « existe-t-il un algorithme général permettant de déterminer si une équation diophantienne (1) admet de solution en nombre entier ? »

Ce problème a été résolu par Yuri Matiasevich en 1970 dans ces travaux, il montra l'impossibilité de trouver une méthode qui résout toutes les équations diophantiennes, ce qui laisse le champ ouvert pour l'étude des équations diophantiennes particulières. Alors, les équations diophantiennes s'étudient indépendamment les unes des autres : si on change un coefficient tout le raisonnement s'écroule et il faut reprendre une nouvelle étude. Ce qui nous ramène à dire qu'il existe des familles d'équations diophantienne qui se traitent de façon uniforme dont l'existence des solution et leurs caractérisations est d'un grand intérêt pour les mathématiciens . En 2012, Karaatli et Siar ont étudié dans [13] l'équation diophantienne $x^2 - kxy + ky^2 + ly = 0$ Pour $l = 2^n$ avec $n \in 0, 1, 2, 3$ et $\in N^*$. Ces auteurs ont déterminé, pour ces différente valeurs de n, les valeurs de k pour lesquelles l'équation admet une infinité de solutions (x,y).

En 2016, dans [22], S.Mavecha a étudie cette famille d'équation pour $l = 2^n$, $n \in \mathbb{N}$ et k un entier impair, et elle a déterminé pour les entiers non négatifs n , les valeurs de k pour lesquelles l'équation admet une infinité de solutions (x,y). De plus, elle a donné une caractérisation de ces solution. Cette étude nous a amené à formuler une généralisation de tout ces travaux, ce qui nous a permi de reformuler d e façon plus précise les résultats fourni par Karaatli et Siar et S.Mavecha. Nous avons établi des résultats pour cette famille d'équations où $l = 2^n$,$n \in N$ et k un entier pair, ainsi que pour $l = 3^n$, $n \in N$ et $k \equiv 2(mod\, 3)$, et pour $l = 2^r \times 3^s$, $r, s \in N$, avec $k = 2k^{'} + 1$ où $k^{'} \equiv 2\,(mod\, 3)$ et .

Dans un sens plus large, on appelle un problème diophantien, la recherche des points entiers ou rationnels sur les courbes algébriques que définissent les équations diophantiennes $p(x, y, z, \ldots\ldots) = 0$. Cette direction donne naissance à notre seconde publication intitulée « Sur l'équation Diophantienne $h(a)x^2 + f(a) = g(a)a^n$ (2) »

Ce travail se décline en quatre parties.

Dans le premier chapitre, on donne des rappels concernant les fractions continues. Ceci nous amène à étudier le développement en fraction continue d'un réelle quadratique. Le deuxième chapitre est consacré aux équation de Pell. On expliquera comment les fractions continues permettent de fournir un moyen rapide et relativement efficace pour le calcul de la solution fondamentale de l'équation de Pell –Fermat$x^2 - dy^2 = 1$. Nous étudierons aussi l'équation générale de Pell $x^2 - dy^2 = N$ pour N dans $\mathbb{Z}$.

Le troisième chapitre s'intitule « sur une équation diophantienne quadratique ».on utilise les congruences et les équations de Pell pour la reformulation et la résolution de certain problème concernant les solutions des équations diophantiennes. On s'intéresse ici, de résoudre des équations diophantienne de la forme $ax^2 + bxy + cy^2 + dx + ey + f = 0$, où a, b, c , d , e "et" f sont des entiers fixés, ce qui est un cas particulier de l'équation (1)

Dans le chapitre 4, le théorème de Siegel nous offre un point de départ permettant de décider de la finitude ou de l'infinitude du nombre de solutions de l'équation (2). Lorsque le théorème de Siegel assure la finitude du nombre de solutions, on s'intéresse à la recherche de ces solutions. Nous utiliserons la théorie des courbes elliptiques et le fameux théorème de Baker sur le nombre de points intégraux sur une courbe elliptique avec les coefficients entiers pour prouver que l'équation (2) n'a que les solutions finies et donner une borne efficace pour ces solutions.

Chapitre 1

Les équations diophantiennes

Afin de nous permettre à résoudre l'équation quadratique

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

nous travaillerons sur la structure de l'anneau d'Euclide $\mathbb{Z}(\sqrt{d})$, d sans facteur carré, muni d'une addition et d'une multiplication, ce qui est au c½ur de l'arithmétique modulaire. Notre équation étant quadratique, alors elle a un lien étroit avec l'équation de Pell généralisé

$$x^2 - dy^2 = N$$

où x et y sont des entiers et où N est un entier non nul fixé, d'où l'intérêt de l'étude et du développement en fractions continues d'un réel quadratique.

1.1 Les fractions continues.

Les fractions continues sont très usitées pour l'approximation des irrationnels par des rationnels, ainsi que pour l'étude de la transcendance. Ceci reste l'outil principal pour le calcul des solutions fondamentales des équations de Pell.

On appelle fraction continue toute expression de la forme

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{\vdots}}}}$$

Où $a_0, a_1, ..., a_n, b_1, b_2, \ldots b_n \in \mathbb{R}^*$ (ou $\mathbb{C}^*$).

Une fraction continue est dite simple si $b_i = 1$, pour $i \geq 1$ et les termes $a_1, ..., a_n$ sont des entiers naturels strictement positifs sauf le premier terme a_0 qui peut être un entier négatif, appelés quotient partiels ou dénominateurs partiels. Dans ce cas, cette fraction continue sera notée $[a_0,\, a_1, ..., a_n, \ldots]$. De plus, si le nombre de termes n est fini la fraction est dite fraction continue finie ou limitée.

1.1.1 Fraction continues finies

Développement en fraction continue d'un nombre rationnel

Théorème 1.1. *la valeur de toute fraction continue finie simple est un nombre rationnel. Réciproquement, tout nombre rationnel peut s'écrire sous forme de fraction continue finie simple*

Démonstration. c'est évident que la valeur de toute fraction continue finie simple est un nombre rationnel car on peut la simplifier en plusieurs étapes pour finalement la ramener à la formea/b avec a et b sont deux entiers relatifs. On montre que tout nombre rationnel a/b , avec $b > 0$, peut s'écrire sous forme de fraction continue finie simple. Pour cela on applique l'algorithme d'Euclide pour chercher le pgcd de a et b.On trouve alors ces équations

$$\begin{aligned}
a &= ba_0 + r_1 \qquad 0 < r_1 < b \\
b &= r_1 a_1 + r_2 \qquad 0 < r_2 < r_1 \\
r_1 &= r_2 a_2 + r_3 \qquad 0 < r < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} a_{n-1} + r_n \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= ba_n + 0
\end{aligned}$$

On remarque que les restes $r_1, r_2\,, r_3, \ldots, r_n$ forment une suite décroissante d'entier positifs majorée dans $\mathbb{N}$ ce qui assure la finitude de l'algorithme précédent, c'est-à-dire que les termes $a_1, a_2, \ldots, a_n$ sont des entiers naturels positifs et le nombre des termes a_i est fini. On récrit cet algorithme , on trouve alors

$$\begin{aligned}
\frac{a}{b} &= a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}} \\
\frac{b}{r_1} &= \frac{r_1.a_1 + r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}} \\
\frac{r_1}{r_2} &= \frac{r_2.a_2 + r_3}{r_2} = a_2 + \frac{1}{\frac{r_2}{r_3}} \\
&\vdots \\
\frac{r_{n-1}}{r_n} &= a_n
\end{aligned}$$

On utilise la deuxième équation pour éliminer le $\frac{b}{r_1}$ dans la première équation, ce qui donne

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\frac{r_1}{r_2}}}$$

et ainsi de suite jusqu'au dernier $\frac{r_{n-1}}{r_n}$, ce qui entraine

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}$$

□

Remarque 1.1. De ce qui précède on remarque

1. Le premier terme a_0 de la fraction continue finie simple $[a_0; a_1, ..., a_n]$ est égal à zéro si la valeur de la fraction continue est un nombre rationnel positif inférieur à 1.
2. La représentation d'un rationnelle en fractions continue n'est pas unique car on peut toujours modifier le dernier terme a_n de la fraction de la façon suivante

$$\frac{1}{a_n} = \frac{1}{a_n - 1 + \frac{1}{1}}$$

   Alors

$$[a_0; a_1, ..., a_n] = [a_0; a_1, ..., a_n - 1, 1]$$

Exemple 1.1. Le développement du nombre $\frac{321}{19}$ en fractions continues fini est donné comme suit

$$\begin{aligned}\frac{321}{19} &= 16+\frac{17}{19}\\ &= 16+\cfrac{1}{\cfrac{19}{17}}\\ &= 16+\cfrac{1}{1+\cfrac{1}{\cfrac{17}{2}}}\\ &= 16+\cfrac{1}{1+\cfrac{1}{8+\cfrac{1}{2}}}\\ &= 16+\cfrac{1}{1+\cfrac{1}{8+\cfrac{1}{1+\cfrac{1}{1}}}}\end{aligned}$$

Par suite, on a

$$\begin{aligned}\frac{321}{19} &= [16,\ 1,\ 8,\ 2]\\ &= [16,\ 1,\ 8,\ 1,\ 1]\,.\end{aligned}$$

1.1.2 Réduite d'une fraction continue finie.

Définition 1.1. On appelle réduite d'ordre k la fraction continue $[a_0; a_1, ..., a_k]$ faite à partir de la fraction $[a_0; a_1, ..., a_n]$, en découpant l'expression après le k-ième dénominateur partiel a_k , $1 \leq k \leq n$. On le note par c_k.

Les réduites de la fraction $[a_0; a_1, ..., a_n]$ sont

$$\begin{aligned}c_0 &= [a_0] = a_0\\ c_1 &= [a_0,\ a_1] = a_0+\frac{1}{a_1} = \frac{a_0a_1+1}{a_1}\\ c_2 &= [a_0,\ a_1, a_2] = a_0+\cfrac{1}{a_1+\cfrac{1}{a_2}} = \frac{a_2\left(a_0a_1+1\right)+a_0}{a_2a_1+1}\\ c_3 &= [a_0,\ a_1, a_2,\ a_3] = a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3}}} = \frac{a_3\left(a_2a_1a_0+a_2+a_0\right)+a_1a_0+1}{a_3a_2a_1+a_1+1}\end{aligned}$$

On définit les suites (p_k) et (q_k) en posant $c_k = \dfrac{p_k}{q_k}$, ce qui donne

$$\begin{array}{lclclcl}
p_0 & = & a_0 & q_0 & = & 1 & \\
p_1 & = & a_1 a_0 + 1 & q_1 & = & a_1 & \\
p_2 & = & a_2 p_1 + p_0 & q_2 & = & a_2 q_1 + q_0 & \\
p_3 & = & a_3 p_2 + p_1 & q_3 & = & a_3 q_2 + q_1 & \\
\vdots & & & \vdots & & & \\
p_k & = & a_k p_{k-1} + p_{k-2} & q_k & = & a_k q_{k-1} + q_k - 2 & \text{pour } k \geq 2
\end{array}$$

Théorème 1.2. *Toute réduite de la fraction continue finie* $[a_0; a_1, ..., a_n]$ *est de valeur* $c_k = \dfrac{p_k}{q_k}$ *où* $p_k = a_k p_{k-1} + p_{k-2}$ *et* $q_k = a_k q_{k-1} + q_{k-2}$ *pourk* ≥ 2 *sous les conditions initiales*

$$\begin{array}{rlrl}
p_0 = & a_0 & q_0 = & 1 \\
p_1 = & a_1 a_0 + 1 & q_1 = & a_1
\end{array}$$

Démonstration. Raisonnons par récurrence sur k, pour $k \geq 2$.
Pour $k = 2$, on vérifie bien que $c_2 = \dfrac{p_2}{q_2}$.
On suppose la relation est vrai pour $k = n$, c'est à dire que $c_n = \dfrac{p_n}{q_n}$. Pour calculer c_{n+1} , il suffit de remplacer a_n par $a_n + \dfrac{1}{a_{n+1}}$ dans l'expression de c_n , d'où l'on obtient

$$\begin{aligned}
c_{n+1} &= \left[a_0; a_1, ..., a_n + \frac{1}{a_{n+1}}\right] \\
&= \frac{\left(a_n + \dfrac{1}{a_{n+1}}\right) p_{n-1} + p_{n-2}}{\left(a_n + \dfrac{1}{a_{n+1}}\right) q_{n-1} + q_{n-2}} \\
&= \frac{a_{n+1}\left(p_{n-1} a_n + p_{n-2}\right) + p_{n-1}}{a_{n+1}\left(q_{n-1} a_n + q_{n-2}\right) + q_{n-1}} \\
&= \frac{a_{n+1} p_n + p_{n-1}}{a_{n+1} q_n + q_{n-1}} = \frac{p_{n+1}}{q_{n+1}}
\end{aligned}$$

□

Exemple 1.2. Reprenons l'exemple de la fraction $\dfrac{321}{19}$ dont une réduite est $[16; 1, 8, 2]$, on aura

$$\begin{array}{lllll} c_0 = & [16] = & \dfrac{p_0}{q_0} = & \dfrac{a_0}{1} = & 16 \\ c_1 = & [16,1] = & \dfrac{p_1}{q_1} = & \dfrac{a_1a_0+1}{a_1} = & \dfrac{1\times 16+1}{1} & = 17 \\ c_2 = & [16,1,8] = & \dfrac{p_2}{q_2} = & \dfrac{a_2p_1+p_0}{a_2q_1+q_0} = & \dfrac{8\times 17+16}{8\times 1+1} & = \dfrac{152}{9} \\ c_3 = & [16,1,8,2] = & \dfrac{p_3}{q_3} = & \dfrac{a_3p_2+p_1}{a_3q_2+q_1} = & \dfrac{2\times 152+17}{2\times 9+1} & = \dfrac{321}{19} \end{array}$$

Proposition 1.1. *Soient (p_n) et (q_n) les deux suites définies par*

$$\begin{array}{llll} p_{-1} = & 1 & q_{-1} = & 0 \\ p_0 = & a_0 & q_0 = & 1 \\ \vdots & & \vdots & \\ p_k = & a_kp_{k-1}+p_{k-2} & q_k = & a_kq_{k-1}+q_{k-2} \quad \text{pour } k \geq 1 \end{array}$$

alors on a

$$1) \quad p_kq_{k-1} - q_kp_{k-1} = (-1)^{k-1} \qquad \text{pour } 0 \leq k \leq n$$

$$2) \quad p_kq_{k-2} - q_kp_{k-2} = (-1)^k a_k \qquad \text{pour } 0 \leq k \leq n$$

$$3) \quad [a_0; a_1, ..., a_k] = \frac{p_k}{q_k} \text{ et } p\gcd(p_k, q_k) = 1 \qquad \text{pour } 0 \leq k \leq n$$

$$4) q_{k-1} \leq q_k \qquad \text{pour } 1 \leq k \leq n$$

$5)a)$ *la suite $c_{2k} = [a_0; a_1, ..., a_{2k}]$ est croissante*

b) la suite $c_{2k+1} = [a_0; a_1, ..., a_{2k+1}]$ est décroissante

c) Toute réduite d'indice pair est plus petite que toute réduite d'indice impaire $c_0 < c_2 < c_4 <$ ....$c_{2n} < c_{2n+1} < \cdots < c_5 < c_3 < c_1$

Démonstration. .

1. ¨Pour $k = 0$, la relation est vérifiée. Par récurrence, on suppose qu'on a $p_kq_{k-1} - q_kp_{k-1} = (-1)^{k-1}$ pour $k = n$ et montrons la relation pour $k = n + 1$.

   En effet, on a

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

2. Pour $0 \leq k \leq n$,

$$\begin{aligned} p_k q_{k-2} - q_k p_{k-2} &= \left(a_k p_{k-1} + p_{k-2}\right) q_{k-2} - \left(a_k q_{k-1} + q_{k-2}\right) p_{k-2} \\ &= a_k \left(p_{k-1} q_{k-2} - q_{k-1} p_{k-2}\right) + q_{k-2} p_{k-2} - q_{k-2} p_{k-2} \end{aligned}$$

   ce qui, par la propriété « 1) », donne

$$p_k q_{k-2} - q_k p_{k-2} = a_k \left(-1\right)^{k-2} = \left(-1\right)^k a_k$$

3. Soit $d = \operatorname{p\,gcd}\left(p_k, q_k\right)$, alors $d \mid \left(p_k q_{k-1} - q_k p_{k-1}\right) = \left(-1\right)^{k-1}$, ce qui implique $d = 1$

4. On a

$$q_1 = a_1 q_0 + q_{-1} = a_1 \geq 1 = q_0.$$

   et pour $n > 0$ on aura

$$q_{n+1} = a_{n+1} q_n + q_{n-1} > a_{n+1} q_n \geq 1 \times q_n.$$

5. De l'égalité $c_{k+2} - c_k = \left(c_{k+2} - c_{k+1}\right) + \left(c_{k+1} - c_k\right)$, on tire

$$\begin{aligned} c_{k+2} - c_k &= \left(\frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}}\right) + \left(\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right) \\ &= \frac{\left(-1\right)^{k+1}}{q_{k+2} q_{k+1}} + \frac{\left(-1\right)^k}{q_{k+1} q_k} \\ &= \frac{\left(-1\right)^k \left(q_{k+2} - q_k\right)}{q_k q_{k+1} q_{k+2}} \end{aligned}$$

   et comme $q_i > 0$, pour tout $i \geq 0$, et sachant que d'après 4) on a $q_{k+2} - q_k > 0$, alors $c_{k+2} - c_k$ est de même signe que $\left(-1\right)^k$, ce qui montre que $c_{2k+2} - c_{2k} > 0$ et donc la suite $\left(c_{2k}\right)$ est croissante et

$$c_{(2k+1)+2} - c_{2k+1} < 0 \Rightarrow \left(c_{2k+1}\right) \text{ est décroissante}$$

   et donc

$$c_{k+1} - c_k = \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{\left(-1\right)^k}{q_k q_{k+1}}$$

   et donc $c_{2k+1} - c_{2k} > 0$

$\square$

1.2 Fractions continues infinies

1.2.1 Propriétés des fractions continues

Les résultats des réduites obtenus pour les fractions continues finies simples restent valides pour les fractions continues infinies simples puisque ces résultats n'ont aucune relation avec la finitude de la fraction.

Théorème 1.3. *Toute fraction continue infinie simple* $[a_0; a_1, a_2, a_3, ...]$ *converge vers une limite* ℓ *qui est la valeur de cette fraction où*

$$\ell = \lim_{n \to +\infty} [a_0; a_1, a_2, a_3, ...a_n].$$

Démonstration. Soit c_k une suite des réduites d'une fraction continue infinie simple $[a_0,\ a_1,\ a_2,\ a_3, ...]$, alors, d'après la propriété 5 de la proposition 1.1 ci-dessus, on a c_{2k} est strictement croissante majorée par c_1 , et c_{2k+1} est strictement décroissante minorée par c_0, alors les suites (c_{2k}) et (c_{2k+1}) sont convergentes et donc il existe deux entiers ℓ et ℓ' tels que

$$\ell = \lim_{n \to +\infty} c_{2n} \text{ et } \ell' = \lim_{n \to +\infty} c_{2n+1}$$

Nous allons montrer que $\ell = \ell'$.

Par le paragraphe précédent on a

$$c_{2k+1} - c_{2k} = \frac{1}{q_{2k}q_{2k+1}}$$

et d'après la propriété 4 de la proposition 1.1, on a

$$c_{2k+1} - c_{2k} < \frac{1}{q_{2k}^2}$$

et sachant que $\lim_{k \to +\infty} q_k = +\infty$, alors les suite (c_{2k+1}) et (c_{2k}) sont adjacentes, ce qui entraine que $\ell = \ell'$.

Par suite, on a :

$$\begin{aligned}
[a_0; a_1, a_2, a_3, ...] &= \lim_{n \to +\infty} [a_0; a_1, a_2, a_3, ...a_n] \\
&= \lim_{n \to +\infty} \left(a_0 + \frac{1}{[a_1, a_2, a_3, ...a_n]} \right) \\
&= a_0 + \lim_{n \to +\infty} \frac{1}{[a_1, a_2, a_3, ...a_n]} \\
&= a_0 + \frac{1}{[a_1, a_2, a_3, ...]}
\end{aligned}$$

□

De plus, on a les résultat suivants

Théorème 1.4. *[25] Si deux fractions continues infinies simples* $[a_0; a_1, a_2, ...]$ *et* $[b_0; b_1, b_2, ...]$ *sont égales alors* $a_n = b_n$ *pour tout* $n \geq 0$.

Théorème 1.5. *Chaque fraction continue infinie simple représente un nombre irrationnel unique, et tout nombre irrationnel peut s'écrire de façon unique sous forme de fractions continues infinies simples.*

Démonstration. Supposons qu'on définit un nombre ℓpar

$$\ell = \lim_{n \to +\infty} [a_0,\, a_1,\, a_2, \ldots, a_n]\,.$$

Si ℓ est rationnel, alors $\ell = \dfrac{a}{b}$, où $a, b \in \mathbb{Z}$ avec $b > 0$. Alors on aura

$$c_{2n} < \frac{a}{b} < c_{2n+1},\ n \in \mathbb{N}$$

par suite

$$0 < \frac{a}{b} - c_{2n} < c_{2n+1} - c_{2n} = \frac{1}{q_{2n}q_{2n+1}}$$

ce qui donne, par multiplication par bq_{2n}

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

Pour n assez grand, on obtient $b < q_{2n+1}$ ce qui entraine

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

C'est-à-dire qu'il existe un nombre naturel non nul inférieur à 1, ce qui est une contradiction !,. Et comme la limite ℓ est unique, on en déduit que chaque fraction continue infinie simple représente un nombre irrationnel unique.

Inversement, on a vue que tout irrationnel x peut s'écrire sous forme de fraction continue de la façon suivante

$$x = [a_0,\, a_1, \ldots, a_n, x_{n+1}]$$

où $x_{n+1} = a_{n+1} + t_{n+1}$ est irrationnel avec $0 < t_{n+1} < 1$.

Si on fixe n, alors les $n + 1$ premières réduites $c_k = \dfrac{p_k}{q_k}$, $0 \leq k \leq n$, de la fraction continue infinie $[a_0,\, a_1, ..., a_n, \ldots]$ sont les mêmes les $n+1$ premières réduites de la fraction continue finie $[a_0; a_1, ..., a_n, x_{n+1}]$. En calculant la réduite d'ordre $n+1$ de la dernière fraction, on trouve

$$c_{n+1} = \frac{a_{n+1}p_n + p_{n-1}}{a_{n+1}q_n + q_{n-1}}$$

En remplaçant a_{n+1} par x_{n+1} dans l'expression de c_{n+1}, on obtient

$$c_{n+1} = \frac{x_{n+1}p_n + p_{n-1}}{xn+1q_n + q_{n-1}}$$

ce qui entraîne

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

Ainsi,

$$\begin{aligned} |x - c_n| &= \frac{1}{\left(x_{n+1}q_n + q_{n-1}\right) q_n} < \frac{1}{\left(a_{n+1}q_n + q_{n-1}\right) q_n} = \frac{1}{q_{n+1}q_n} \\ &< \frac{1}{q_n^2} \underset{n\to\infty}{\longrightarrow} 0\,. \end{aligned}$$

Par conséquent,

$$x = \lim_{n\to+\infty} c_n = [a_0,\, a_1, \ldots, a_n, \ldots]$$

C'est à-dire que toute réduite $c_n = \dfrac{p_n}{q_n}$ approche x à moins de $\dfrac{1}{q_n^2}$ près. □

Lemme 1.1. *Soit x un irrationnel et soit $\frac{p_n}{q_n}$ la réduite d'ordre n de la fraction continue qui représente x. S'il existe deux entiers a et b tels que $1 < b < q_{n+1}$ alors*

$$|q_n x - p_n| \leq |bx - a|$$

Démonstration. Soit x un irrationnel et soit $\dfrac{p_n}{q_n}$ et $\dfrac{p_{n+1}}{q_{n+1}}$ les réduites d'ordre n et $n+1$ de la fraction continue de x, soit a et b des entiers tels que $1 < b < q_{n+1}$. On considère le système d'équations suivant :

$$\begin{cases} p_n\alpha + p_{n+1}\beta &= a \\ q_n\alpha + q_{n+1}\beta &= b \end{cases}$$

Ce système d'inconnue (α,β) a pour déterminant $p_nq_{n+1}-q_np_{n+1}=(-1)^{n+1}\neq 0$, ce qui implique l'existence d'une solution unique donnée par

$$(\alpha,\beta)=\Big((-1)^{n+1}\left(aq_{n+1}-bp_{n+1}\right)\ ,\ (-1)^{n+1}\left(bp_n-aq_n\right)\Big)$$

— Si $\alpha=0$, alors $aq_{n+1}=bp_{n+1}$ et comme $pgcd(p_{n+1},q_{n+1})=1$ on aura $q_{n+1}\mid b$ ce qui implique qu'$\exists r\in\mathbb{Z}$ tel que $b=rq_{n+1}$, d'où $b>q_{n+1}$ ce qui contredit notre hypothèse et donc $\alpha\neq 0$.

— Si $\beta=0$, alors $a=p_n\alpha$ et $b=q_n\alpha$ et on a

$$|bx-a|=|q_n\alpha x-p_n\alpha|=|\alpha|\,|q_nx-p_n|\geq|q_nx-p_n|$$

— On suppose dans ce qui suite $\beta\neq 0$. Montrons que dans ce cas, α et β sont de signes contraires.

  — Si $\beta<0$ avec $q_n\alpha=b-q_{n+1}\beta$,$b>0$ et $q_n>0$, d'où l'on obtient $\alpha>0$.

  — Si $\beta>0$, avec $0<b<q_{n+1}$, alors $0<b<\beta b<\beta q_{n+1}$ et entraine que $q_n\alpha=b-\beta q_{n+1}<0$ et donc $\alpha<0$.

Comme $x$est compris entre deux réduites successive, alors

$$\frac{p_n}{q_n}<x<\frac{p_{n+1}}{q_{n+1}}$$

il s'ensuit que

$$q_nx-p_n>0 \text{ et } q_{n+1}x-p_{n+1}<0$$

Ainsi, les nombres $\alpha\left(q_nx-p_n\right)$ et $\beta\left(q_{n+1}x-p_{n+1}\right)$ sont de même signe et cela entraine que

$$\left|\alpha\left(q_nx-p_n\right)+\beta\left(q_{n+1}x-p_{n+1}\right)\right|=\left|\alpha\left(q_nx-p_n\right)\right|+\left|\beta\left(q_{n+1}x-p_{n+1}\right)\right|$$

Par suite, on aura

$$\begin{aligned}|bx-a|&=\left|\left(q_n\alpha+q_{n+1}\beta\right)x-\left(p_n\alpha+p_{n+1}\beta\right)\right|\\&=\left|\alpha\left(q_nx-p_n\right)+\beta\left(q_{n+1}x-p_{n+1}\right)\right|\\&=\left|\alpha\left(q_nx-p_n\right)\right|+\left|\beta\left(q_{n+1}x-p_{n+1}\right)\right|\\&\geq|\alpha|\,|q_nx-p_n|\\&\geq|q_nx-p_n|\,.\end{aligned}$$

□

Théorème 1.6. *[?]*
soit x un nombre irrationnel et soit $\frac{a}{b}$ un nombre rationnel avec $b \geq 1$ et $pgcd(a,b) = 1$. Si le rationnel $\frac{a}{b}$ réalise

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

alors $\frac{a}{b}$ est l'une des réduites de la fraction continue représentant x.

Démonstration. supposons que $\frac{a}{b}$ n'est pas une réduites de la fraction continue qui représente x tel que

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2} \text{ avec } b \geq 1$$

Comme les dominateurs q_k des réduites forment une suite strictement croissante, alors il existe un entier n tel que

$$1 \leq q_n \leq b \leq q_{n+1}$$

et par le Lemme précédent on aura

$$|q_n x - p_n| \leq |bx - a| = b\left|x - \frac{a}{b}\right| < \frac{1}{2b}.$$

ce qui donne

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

et par suite

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

Comme on a $\frac{a}{b} \neq \frac{p_n}{q_n}$ pour tout entier naturel n, alors

$$|bp_n - aq_n| \geq 1$$

d'où l'on tire

$$\frac{1}{bq_n} \leq \frac{|bp_n - aq_n|}{bq_n} = \left|\frac{p_n}{q_n} - \frac{a}{b}\right|.$$

D'autre part, nous avons

$$\left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\frac{p_n}{q_n} - x\right| + \left|x - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}$$

ce qui implique que

$$\frac{1}{bq_n} < \frac{1}{2bq_n} + \frac{1}{2b^2}$$

ce qui donne

$$\frac{1}{2bq_n} < \frac{1}{2b^2}$$

et comme $b > 0$, on obtient

$$\frac{1}{q_n} < \frac{1}{b}$$

ce qui contredit $q_n < b < q_{n+1}$. □

1.3 Fractions continues périodiques

Définition 1.2. Une fraction continue $[a_0; a_1, ...]$ est dite périodique à partir d'un certain rang $n_0 \geq 0$ s'il existe un entier $t \geq 1$ tel que $\forall i \geq n_0$ on a $a_i = a_{t+i}$. Dans ce cas, l'entier t est appelé longueur de la période.

Dans le cas d'une fraction continue périodique, cas, celle-ci s'écrit

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

et on la note

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

Définition 1.3. Une fraction continue est dite purement périodique si elle est de la forme

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

pour un certain entier n_0.

Le résultat suivant donne une caractérisation des nombres irrationnels quadratiques moyennant leurs développements en fractions continues.

Théorème 1.7. *[25]*
Une fraction continue est périodique si est seulement si elle représente un nombre irrationnel quadratique. Si d est un entier positif sans facteur carré, alors le développement en fraction continue de $\sqrt{d}$ est

$$[a_0, \overline{a_1, \ldots a_{t-1}, 2a_0}]$$

où $a_0 = \left[\sqrt{d}\right]$.

Théorème 1.8. *[30]*

Soit x un nombre réel quadratique et notons $\overline{x}$ son conjugué , alors le développement en fractions continues de x est purement périodique si et seulement si $x > 1$ et $-1 < \overline{x} < 0$.

En fait, dès qu'un nombre algébrique β est de degré $n > 2$, on ne sait pas grand-chose sur son développement en fraction continue, tel que la périodicité, le lien des éléments du développement avec le degré , et l'ordre de grandeur des éléments du développement.

Lemme 1.2. *[30]*

Soit d un entier positif non carré parfait, et soit $[a_0; \overline{a_1, ...a_{l-1}, a_l}]$, le développement de $\sqrt{d}$ en fraction continue de longueur minimale de la période l, et soit $c_k = \frac{p_k}{q_k}$ la réduite d'ordre k de cette fraction alors

$$p_{kl-1}^2 - dq_{kl-1}^2 = (-1)^{kl}, \quad k = 1, 2, \ldots$$

Chapitre 2

Equations de Pell

Soit d un entier strictement positive non carré parfait et N un entier non nul.
L'équation diophantienne $x^2 - dy^2 = N$ est appelée équation de pell généralisée, et nous désignons indifféremment par (x, y) ou $x + y\sqrt{d}$ une solution de cette équation. De plus, si x et y sont tout deux strictement positifs, nous dirons que $x + y\sqrt{d}$ est une solution positive de l'équation de Pell généralisée. Deux solutions $x_1 + y_1\sqrt{d}$ et $x_2 + y_2\sqrt{d}$ sont dites égales si $x_1 = x_2$ et $y_1 = y_2$. Pour $N = +1$, on retrouve l'équation classique de Pell $x^2 - dy^2 = 1$ appelée équation positive de Pell. Pour $N = -1$, on aura l'équation $x^2 - dy^2 = -1$ appelé équation négative de Pell, qui elle n'a pas toujours de solution. En effet, en considérant l'équation de Pell : $x^2 - 3y^2 = -1$ n'admet pas de solution, et pour le constater, il suffit de supposer qu'elle en admette une, on aurait la congruences $x^2 \equiv 2\,(mod 3)$, ce qui est impossible puisque 2 n'est pas un carré dans $\mathbb{F}_3$. En utilisant cette idée, il est facile de constater que si d est un entier tel que $d \equiv 3\,(\text{mod } 4)$, l'équation $x^2 - dy^2 = -1$ ne possède pas de solution puisque dans $\mathbb{Z}/4\mathbb{Z}$ l'équation s'écrit $x^2 + y^2 = -1$ alors que dans $\mathbb{Z}/4\mathbb{Z}$ x^2 et $y^2 \not\equiv -1 \;(\text{mod } 4)$.

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

Résoudre l'équation de Pell-Fermat $x^2 - dy^2 = 1$ revient à trouver un entier y tel que $1 + dy^2$ soit un carré parfait, sachant que $(x = \pm 1, y = 0)$ sont des solution triviales de cette équation.
L'ensemble des solutions de l'équation $x^2 - dy^2 = 1$ est fini dans les cas suivants :

— Pour$d < -1$, l'équation $x^2 - dy^2 = 1$ n'admet pas de solution en dehors des solutions triviales $(-1, 0)$ et $(1, 0)$.

— Pour $d = -1$, l'équation s'écrit $x^2 + y^2 = 1$ dont les solutions sont $(\pm 1, 0)$ et $(0, \pm 1)$.

— Pour d un carré parfait, $d = n^2$ pour $n \in \mathbb{N}^*$, alors l'équation de Pell s'écrit

$$(x - ny)\,(x + ny) = 1$$

alors

$$(x - ny) \text{ et } (x + ny) \in \{-1, 1\}$$

et d'autre part, on a

$$x = \frac{(x + ny) + (x - ny)}{2}$$

Sachant que dans le cas cas où $x = 0$ on aura $n^2y^2 = -1$ ce qui est absurde, alors on aura nécessairement

$$x - ny = x + ny$$

ce qui donne $x = \pm 1$ et donc $y = 0$. Par conséquent, l'équation de Pell $x^2 - dy^2 = 1$, pour d un carré parfait, admet pour seules solutions $(-1, 0)$ et $(1, 0)$.

— Pour d entier positif non carré parfait, et en remarquant que

$$\left(r^2 + d\right)^2 - d\,(2r)^2 = \left(r^2 - d\right)^2$$

on peut poser

$$x = \frac{r^2 + d}{r^2 - d} \text{ et } y = \frac{2r}{r^2 - d}$$

avec $x, y \in \mathbb{Q}$ vérifiant

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

ce qui montre que l'équation de Pell admet une infinité de solutions dans $\mathbb{Q}$. Trouver parmi ces solutions celle qui sont dans $\mathbb{Z}$ revient à rechercher les élément α dans $\mathbb{Z}\left[\sqrt{d}\right] = x + y\sqrt{d}$, avec $x, y \in \mathbb{Z}$ tel que $N(\alpha) = 1$, où N désigne l'application norme définie par

$$\begin{aligned} N \ : \qquad \mathbb{Z} \qquad & \longrightarrow \mathbb{Z} \\ \alpha = x + y\sqrt{d} \quad & \longrightarrow N\,(\alpha) \quad = x^2 - dy^2 \end{aligned}$$

Les éléments α de l'anneau $\mathbb{Z}\left[\sqrt{d}\right]$ avec $N\,(\alpha) = \pm 1$ sont les unités de l'anneau $\mathbb{Z}\left[\sqrt{d}\right]$.
Si (x, y) est une solution positive de l'équation $x^2 - dy^2 = \pm 1$,, alors $(-x)^2 + d\,(-y)^2 = \pm 1$. Ainsi, pour trouver les solutions de l'équations de cette équation de Pell, il suffit de trouver ses solutions positifs.

Proposition 2.1. *si $x_1 + y_1\sqrt{d}et$ $x_2 + y_2\sqrt{d}$ sont deux solutions positives de l'équation*

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

alors les assertions suivantes sont équivalentes

1. $x_1 < x_2$,

2. $y_1 < y_2$,

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

Démonstration. Commençons par la remarque suivante , puisque x_1, x_2, y_1 et y_2 sont positifs,

$$x_1 < x_2 \Leftrightarrow x_1^2 < x_2^2 \Leftrightarrow x_1^2 - 1 < x_2^2 - 1 \Leftrightarrow y_1^2 < y_2^2 \Leftrightarrow y_1 < y_2$$

ce qui montre que les deux premières assertions sont équivalentes.
D'une part, si $x_1 + y_1\sqrt{d}$et $x_2 + y_2\sqrt{d}$ sont deux solutions positives de l'équation $x^2 - dy^2 = 1$, alors

$$x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = 1$$

ce qui donne

$$(x_2 - x_1)(x_2 + x_1) = \sqrt{d}(y_2 - y_1)\sqrt{d}(y_2 + y_1).$$

et par suite $(x_2 - x_1)$ et $(y_2 - y_1)$ sont de même signe, puisque x_1, x_2, y_1 et y_2 sont positifs.
D'autre part, l'hypothèse $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$ implique que $(x_2 - x_1) + (y_2 - y_1)\sqrt{d} > 0$, ce qui entraine nécessairement $x_2 - x_1 > 0$ et $y_2 - y_1 > 0$, en d'autre termes on a $x_1 < x_2$ et $y_1 < y_2$.
Inversement, si $x_1 < x_2 \Leftrightarrow y_1 < y_2$ alors $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$ □

Théorème 2.1. *Étant donné un entier positif d qui ne soit pas un carré parfait, on considère l'ensemble S des solutions positives de l'équation $x^2 - dy^2 = 1$. Si $S \neq \emptyset$, alors*

1. *S est infini, ordonné et dénombrable.*

2. *S possède un plus petit élément $\alpha = x_1 + y_1\sqrt{d}$, pour $d > 1$.*

Démonstration. Soit (x, y) une solution positive de l'équation de Pell $x^2 - dy^2 = 1$.

1. Si $x + y\sqrt{d}$ est une solution non triviale de l'équation $x^2 - dy^2 = 1$, alors on a $\left(x^2 - dy^2\right)^2 = 1$ et donc $\left(x^2 + dy^2\right)^2 - d(2xy)^2 = 1$. Ainsi, $\left(x^2 + dy^2, 2xy\right)$ est aussi solution de cette équation qui est strictement supérieure à $x + y\sqrt{d}$. On construit ainsi, une suite de solutions strictement croissante ce qui permet d'affirmer que l'équation $x^2 - dy^2 = 1$ possède une infinité de solution. D'autre part on a $S \subset \mathbb{N} \times \mathbb{N}$ et $\mathbb{N} \times \mathbb{N}$ est dénombrable ce qui sera le cas de S.

2. D'après la proposition 2.1, on peut ordonner les éléments de S suivant l'ordre croissant de x, ou selon l'ordre croissant des y , ou encore selon l'ordre croissant des $x + y\sqrt{d}$, puisque c'est

le même ordre. Ainsi, S possède donc un plus petit élément $\alpha = x_1 + y_1\sqrt{d}$ et comme $\sqrt{d} > 1$, $x_1 > 0$ et $y_1 > 0$ alors $\alpha > 1$.

□

Définition 2.1. La solution minimale positive de l'équation $x^2 - dy^2 = 1$ est appelée solution fondamentale.

La détermination de la solution fondamentale de l'équation de Pell $x^2 - dy^2 = 1$ n'est pas toujours facile, parce que les solutions de l'équation peuvent être grandes, c'est le cas notamment d l'équation $x^2 - 99y^2 = 1$ dont la solution fondamentale est $\alpha = x_1 + y_1\sqrt{d}$:

$$x_1 = 379516400906811930638014896080$$

$$x_2 = 12055735790337 - 1447442538767$$

Théorème 2.2. *Soit $\alpha = x_1 + y_1\sqrt{d}$ la solution fondamentale de l'équation de Pell*

$$x^2 - dy^2 = 1 \tag{2.1}$$

alors l'ensemble T de ses solutions pour $x > 0$ et $y > 0$ est

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

où

$$\begin{cases} x_n = & x_1^n + \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \begin{pmatrix} n \\ 2k \end{pmatrix} x_1^{n-2k} y_1^{2k} d^k \\ y_n = & \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} \begin{pmatrix} n \\ 2k-1 \end{pmatrix} x_1^{n-2k+1} y_1^{2k-1} d^{k-} \end{cases}$$

de plus les suite (x_n) et (y_n) vérifient les relations de récurrence suivantes

1. $x_{n+1} = x_1 x_n + dy_1 y_n$ *et* $y_{n+1} = y_1 x_n + x_1 y_n$
2. $x_{n+1} = 2x_1 x_n - x_{n-1}$ *et* $y_{n+1} = 2y_1 x_n - y_{n-1}$
3. $x_n = \dfrac{\alpha^n + \overline{\alpha}^n}{2}$ *et* $y_n = \dfrac{\alpha^n - \overline{\alpha}^n}{2\sqrt{d}}$

Démonstration. Soit S l'ensemble des solution de l'équation de Pell (2.1) et T l'ensemble de solutions positives de l'équation de Pell (2.1), alors

$$T = \left\{x_n + y_n\sqrt{d},\, n \in \mathbb{N}^*\right\} = \left\{\left(x_1 + y_1\sqrt{d}\right)^n,\, n \in \mathbb{N}^*\right\} \tag{2.2}$$

Où $x_1 + y_1\sqrt{d}$ est solution de l'équation de Pell. Sachant que le conjugué d'un produit est produit des conjugués, alors

$$x_n - y_n\sqrt{d} = \left(x_1 - y_1\sqrt{d}\right)^n \tag{2.3}$$

Sachant que $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$ et par multiplication membres à membres des équations (2.2) et (2.3), on obtient

$$x_n^2 - dy_n^2 = \left(x_1^2 - dy_1^2\right)^n = 1$$

et comme $x_1$et y_1 sont des entiers positifs, alors x_n et y_n sont aussi des entiers positifs ce qui montre que $x_n + y_n\sqrt{d} \in T$ ainsi $T \subsetneqq S$. Supposons que T est strictement inclus dans S, alors il existe un élément $u + v\sqrt{d} \in S$ avec $u + v\sqrt{d} \notin T$. Comme les éléments de T constituent une suite strictement croissante, il existe $n_0 \in \mathbb{N}^*$ tel que

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

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

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

ce qui donne

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

En posant

$$\left(u + v\sqrt{d}\right)\left(x_{n_0} - y_{n_0}\sqrt{d}\right) = \left(ux_{n_0} - y_{n_0}vd\right)\left(x_{n_0}v - y_{n_0}u\right)\sqrt{d} = r + s\sqrt{d} \tag{2.4}$$

on aura

$$\left(u - v\sqrt{d}\right)\left(x_{n_0} + y_{n_0}\sqrt{d}\right) = r - s\sqrt{d} \tag{2.5}$$

et

$$1 < r + s\sqrt{d} < x_1 + y_1\sqrt{d} \tag{2.6}$$

Par multiplication des expression (.2.4.) et (2.5), on obtient

$$1 = \left(u^2 - dv^2\right)\left(x_{n_0}^2 - dy_{n_0}^2\right) = r^2 - ds^2 \tag{2.7}$$

Sachant que la relation (2.6) donne

$$0 < r - s\sqrt{d} = \frac{1}{r + s\sqrt{d}} < 1 \tag{2.8}$$

alors les dernière relations (2.6) et (2.8) donnent $r > 0$ et $s > 0$.

En vertu du fait que $r + s\sqrt{d}$ est solution positive de l'équation de Pell (2.1) , $r > 0$ et $s > 0$, et que $r + s\sqrt{d} < x_1 + y_1\sqrt{d}$ ce qui, par minimalité de $x_1 + y_1\sqrt{d}$, est impossible, ce qui montre que $T = S$

1. On a

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

   ce qui donne

$$\begin{cases} x_{n+1} = x_1 x_n + d y_1 y_n \\ y_{n+1} = y_1 x_n + x_1 y_n \end{cases} \tag{2.9}$$

2. D'autre part, on a

$$\begin{cases} x_{n+1} = x_1 x_n + d y_1 y_n = 2x_1 x_n - (x_1 x_n - d y_1 y_n) \\ y_{n+1} = y_1 x_n + x_1 y_n = 2y_1 x_n - (y_1 x_n - x_1 y_n) \end{cases}$$

   Et comme on a

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

   il en résulte que

$$\begin{cases} x_{n+1} = 2x_1 x_n - x_{n-1} \\ y_{n+1} = 2y_1 x_n - y_{n-1} \end{cases} .$$

3. La relation (2.9) peut s'écrire sous la forme

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

ce qui donne par récurrence

$$\begin{aligned} \begin{pmatrix} x_n \\ y_n \end{pmatrix} &= \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ y_{n-1} \end{pmatrix} \\ &= \begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}^{n-1} \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} \end{aligned} \tag{2.10}$$

La matrice $\begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix}$ admet pour valeurs propres $\alpha = x_1 + y_1\sqrt{d}$ et $\overline{\alpha} = x_1 - y_1\sqrt{d}$ dont les vecteurs propres correspondants sont $V_\alpha = \begin{pmatrix} 1 \\ \frac{1}{\sqrt{d}} \end{pmatrix}$ et $V_{\overline{\alpha}} = \begin{pmatrix} -\sqrt{d} \\ 1 \end{pmatrix}$.

Comme $\alpha \neq \overline{\alpha}$, alors les vecteurs V_α et $V_{\overline{\alpha}}$ sont linéairement indépendants, ce qui montre que

$$\begin{pmatrix} x_1 & dy_1 \\ y_1 & x_1 \end{pmatrix} = P \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix} P^{-1} \text{ où } P = \begin{pmatrix} 1 & -\sqrt{d} \\ \frac{1}{\sqrt{d}} & 1 \end{pmatrix}$$

et on a $P^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{\sqrt{d}}{2} \\ \frac{-1}{2\sqrt{d}} & \frac{1}{2} \end{pmatrix}$.

Par suite, on aura

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

et la relation (2.10) devient

$$\begin{aligned} \begin{pmatrix} x_n \\ y_n \end{pmatrix} &= \begin{pmatrix} \frac{\alpha^{n-1}}{2}\left(x_1 + y_1\sqrt{d}\right) + \frac{\overline{\alpha}^{n-1}}{2}\left(x_1 - y_1\sqrt{d}\right) \\ \frac{\alpha^{n-1}}{2\sqrt{d}}\left(x_1 + y_1\sqrt{d}\right) - \frac{\overline{\alpha}^{n-1}}{2\sqrt{d}}\left(x_1 - y_1\sqrt{d}\right) \end{pmatrix} \\ &= \begin{pmatrix} \frac{\alpha^n+\overline{\alpha}^n}{2} \\ \frac{\alpha^n+\overline{\alpha}^n}{2\sqrt{d}} \end{pmatrix}. \end{aligned}$$

□

Théorème 2.3. *soit d un entier positif qui n'est pas un carré parfait. Si x_1 et y_1 sont des nombres naturels satisfaisant l'inégalité*

$$x_1 > \frac{y_1^2}{2} - 1 \tag{2.11}$$

et si $\alpha = x_1 + y_1\sqrt{d}$ est une solution de l'équation Pell $x^2 - dy^2 = 1$, alors α est la solution fondamentale de cette équation de Pell.

Démonstration. pour $y_1 = 1$, le Théorème est évident.

Supposons maintenant que $y_1 > 1$, et que $X + Y\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$ et on suppose en outre que $1 \leq Y \leq y_1$.

Nous avons

$$X^2 - dY^2 = 1 = x_1^2 - dy_1^2$$

alors

$$\frac{X^2 - 1}{Y^2} = \frac{x_1^2 - 1}{y_1^2} = d$$

et posons

$$y_1^2 X^2 - Y^2 x_1^2 = y_1^2 - Y^2.$$

alors on a

$$(y_1 X + Y x_1)(y_1 X - Y x_1) = y_1^2 - Y^2$$

Posons $\delta = (y_1 X + Y x_1)(y_1 X - Y x_1)$, $\delta_1 = (y_1 X + Y x_1)$ et $\delta_2 = (y_1 X - Y x_1)$. Comme $y_1^2 - Y^2 > 0$ et par hypothèse on a $\delta_1 > 0$, alors $\delta_2 > 0$ et donc δ_1 et δ_2 sont des entiers naturels tels que $\delta = \delta_1 \delta_2$. On en tire alors

$$x_1 = \frac{\delta_1 - \delta_2}{2Y} \leq \frac{\delta - 1}{2Y}$$

puisque $\delta_1 - (\delta_2 - 1) \leq \delta$, et on a

$$\frac{\delta - 1}{2Y} = \frac{y_1^2 - \left(Y^2 + 1\right)}{2Y}.$$

Sachant que $Y \geq 1$, alors $2Y \geq 2$ et $Y^2 + 1 \geq 2$, alors

$$x_1 \leq \frac{1}{2} y_1^2 - 1$$

ce qui contredit (2.11), nous devons donc avoir $Y = y_1$ comme affirmé dans le Théorème 2.3. $\square$

2.2 L'équation de Pell $x^2 - dy^2 = -1$.

Trouver les solutions de $x^2 - dy^2 = -1$ dans $\mathbb{Z}$, revient à trouver les éléments $\beta \in \mathbb{Z}\left[\sqrt{d}\right]$ tels que $N(\beta) = -1$, où N désigne l'application norme. Contrairement à l'équation précédente de Pell $x^2 - dy^2 = -1$ précédente, cette équation ne possède pas toujours de solution entière sauf pour certaines valeur de d. Mais si elle en a une, elle en a une infinité.

— Si $d \leq -1$, alors $-d \geq 1$ ce qui implique que

$$x^2 - dy^2 \geq x^2 + y^2 \geq 0.$$

Donc l'équation $x^2 - dy^2 = -1$ n'admet pas de solutions entières.

— Si $d = 0$, alors on trouve $x^2 = -1$, donc l'équation $x^2 - dy^2 = -1$ n'admet pas de solutions entières.

— Si $d = n^2$ avec$n \in \mathbb{N}^*$, alors notre équation devient

$$x^2 - ny^2 = -1$$

ce qui équivaut à $x^2 = (ny)^2 - 1$.

  — Si $ny = 1$, alors $x = 0$ et dans ce cas la solution de l'équation est $(0, 1)$ si $n = 1$ et $(0, -1)$ si $n = -1$.

  — Si $ny = -1$, alors $x = 0$, ce qui donne $(0, 1)$ ou $(0, -1)$ pour solution de l'équation selon que $n = -1$ ou $n = 1$.

  — Si $|ny| \neq 1$, alors l'équation $x^2 = (ny)^2 - 1$ n'admet pas de solution entière.

Les condition nécessaire de résolubilité de l'équation de Pell $x^2 - dy^2 = -1$ sont données par

Proposition 2.2. *[25] Supposons que l'équation $x^2 - dy^2 = -1$ possède des solutions alors*

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

Ces deux conditions ne sont pas suffisantes comme montrera l'exemple suivant :

Exemple 2.1. Considérons l'équation de Pell

$$x^2 - 34y^2 = -1$$

Le nombre 34 est pair et est de la forme $4k+2$, et on a aussi $34 = 2 \times 17$ et $17 = 4\ell + 1$ ce qui assure les conditions nécessaires de la proposition précédente, par contre l'équation de Pell $x^2 - 34y^2 = -1$ n'admet pas de solution.

En effet, si l'équation admettait une solution alors sa solution fondamentale est de la forme $x_1 + y_1\sqrt{34}$ ce qui implique que $\left(x_1 + y\sqrt{34}\right)^2$ serait la solution fondamentale de l'équation $x^2 - 34y^2 = 1$ et qui est $35 + 6\sqrt{34}$. Par suite, on aura

$$\begin{cases} x_1^2 + 34y_1^2 = 35 \\ x_1 y_1 = 3 \end{cases}$$

Mais ce dernier système d'équation ne possède pas de solution dans $\mathbb{N}$, et par conséquent l'équation $x^2 - 34y^2 = -1$ n'admet pas de solution.

Théorème 2.4. *Soit d un entier naturel qui n'est pas un carré parfait.*

Supposons que l'équation $x^2 - dy^2 = -1$ est résoluble, et soit $u_1 + v_1\sqrt{d}$ sa solution fondamentale. Alors

1. $x_1 + y_1\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^2 = \left(u_1^2 + dv_1^2\right) + (2u_1v_1)\sqrt{d}$ *est la solution fondamentale de l'équation* $x^2 - dy^2 = 1$.
2. *Toutes les solutions entières positives de l'équation $x^2 - dy^2 = -1$ sont données par* $u_n + v_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^{2n-1}, n \in \mathbb{N}^*$.
3. *Toutes les solutions entières positives de l'équation $x^2 - dy^2 = 1$ sont données par* $x_n + y_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^{2n}, n \in \mathbb{N}^*$

Démonstration. Considérons l'équation de Pell $x^2 - dy^2 = -1$.

1. Posons

$$\begin{aligned} a + b\sqrt{d} &= \left(u_1 + v_1\sqrt{d}\right)^2 \\ &= \left(u_1^2 + dv_1^2\right) + (2u_1v_1)\sqrt{d} \end{aligned}$$

alors

$$\begin{aligned} a^2 - db^2 &= \left(u_1^2 + dv_1^2\right)^2 - d\,(2u_1v_1)^2 \\ &= u_1^4 + dv_1^4 - 2du_1^2v_1^2 \\ &= \left(u_1^2 - dv_1^2\right)^2 = (-1)^2 = 1 \end{aligned}$$

Ce qui nous permet d'affirmer que $a + b\sqrt{d}$ est la solution de l'équation $x^2 - dy^2 = 1$. Comme

$x_1 + y_1\sqrt{d}$ est la solution de cette équation, alors

$$1 < x_1 + y_1\sqrt{d} < a + b\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^2. \tag{2.12}$$

On a $u_1^2 - dv_1^2 = -1$, alors

$$\left(u_1 - v_1\sqrt{d}\right)\left(u_1 + v_1\sqrt{d}\right) = -1$$

ce qui donne

$$u_1 - v_1\sqrt{d} = \frac{-1}{u_1 + v_1\sqrt{d}} < 0.$$

En multipliant l'inégalité (2.12) par $v_1\sqrt{d} - u_1$, on obtient

$$v_1\sqrt{d} - u_1 < \left(x_1 + y_1\sqrt{d}\right)\left(v_1\sqrt{d} - u_1\right) < \left(u_1 + v_1\sqrt{d}\right)^2\left(v_1\sqrt{d} - u_1\right) \tag{2.13}$$

et on a

$$\left(u_1 + v_1\sqrt{d}\right)^2\left(v_1\sqrt{d} - u_1\right) = -\left(u_1^2 - dv_1^2\right)\left(u_1 + v_1\sqrt{d}\right) = u_1 + v_1\sqrt{d}.$$

Donc l'inégalité (2.13) devient

$$v_1\sqrt{d} - u_1 < \left(x_1 + y_1\sqrt{d}\right)\left(v_1\sqrt{d} - u_1\right) < u_1 + v_1\sqrt{d} \tag{2.14}$$

Soit $u + v\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)\left(v_1\sqrt{d} - u_1\right)$, alors

$$u + v\sqrt{d} = (dy_1v_1 - x_1u_1) + (x_1v_1 - y_1u_1)\sqrt{d}$$

ce qui entraine

$$\begin{aligned} u^2 - dv^2 &= (dy_1v_1 - x_1u_1)^2 - d(x_1v_1 - y_1u_1)^2 \\ &= x_1^2\left(u_1^2 - dv_1^2\right) - dy_1^2\left(u_1^2 - dv_1^2\right) \\ &= \left(u_1^2 - dv_1^2\right) - \left(x_1^2 - dy_1^2\right) \\ &= (-1) \times 1 = -1. \end{aligned}$$

Alors (u, v) est solution de l'équation $x^2 - dy^2 = -1$ avec $u + v\sqrt{d} > 0$. Il reste à montrer que u et v sont strictement positif.

En passant à l'inverse dans la relation (2.14), on obtient

$$0 < \frac{1}{u_1 + v_1\sqrt{d}} \leq \frac{1}{u + v\sqrt{d}} < \frac{1}{v_1\sqrt{d} - u_1}$$

ce qui entraine

$$0 < \frac{u_1 - v_1\sqrt{d}}{u_1^2 - dv_1^2} \leq \frac{u - v\sqrt{d}}{u^2 - dv^2} < \frac{v_1\sqrt{d} + u_1}{dv_1^2 - u_1^2}$$

Sachant que (u, v) et (u_1, v_1) sont respectivement une solution et la solution fondamentale de $x^2 - dy^2 = -1$, on aura

$$0 \leq -\left(u_1 - v_1\sqrt{d}\right) \leq -\left(u - v\sqrt{d}\right) < v_1\sqrt{d} + u_1 \tag{2.15}$$

ce qui donne

$$0 < v_1\sqrt{d} - u_1 \leq v\sqrt{d} - u < u_1 + v_1\sqrt{d} \tag{2.16}$$

Par addition des inégalités (2.14) et (2.16), on obtient

$$0 < 2\left(v_1\sqrt{d} - u_1\right) \leq 2v\sqrt{d} \leq 2\left(u_1 + v_1\sqrt{d}\right)$$

et l'on déduit que $v > 0$.
Comme $u + v\sqrt{d}$ est solution de l'équation $x^2 - dy^2 = -1$ alors $-u + v\sqrt{d}$ est aussi solution de cette équation, avec $0 < -u + v\sqrt{d} < u_1 + v_1\sqrt{d}$ d'après (2.15), et si u est négatif alors on tombe sur une contradiction avec la définition de $u_1 + v_1\sqrt{d}$, donc u est strictement positif.
La définition de $u_1 + v_1\sqrt{d}$ nous donne

$$u_1 + v_1\sqrt{d} < u + v\sqrt{d}$$

et par (2.14) on en conclut

$$u_1 + v_1\sqrt{d} = u + v\sqrt{d}$$

Par définition de $u_1 + v_1\sqrt{d}$, on obtient

$$u_1 + v_1\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)\left(v_1\sqrt{d} - u_1\right)$$

ce qui implique que

$$\begin{aligned} x_1 + y_1\sqrt{d} &= \left(u_1 + v_1\sqrt{d}\right)\frac{-1}{u_1 - v_1\sqrt{d}} \\ &= \left(u_1 + v_1\sqrt{d}\right)^2 \end{aligned}$$

2. Supposons qu'il existe une solution positive $u + v\sqrt{d}$ de l'équation $x^2 - dy^2 = -1$ qui n'est pas donnée par la formule $u_n + v_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^{2n-1}$.
Comme $u_1 + v_1\sqrt{d} > 1$ alors $\left(u_1 + v_1\sqrt{d}\right)^{2n-1}$ est très grand, c'est-à-dire que nécessairement $u + v\sqrt{d}$ est entre deux puissances successives de $u_1 + v_1\sqrt{d}$ puisque $u_n + v_n\sqrt{d}$ forment une suite croissante, on a donc

$$\left(u_1 + v_1\sqrt{d}\right)^{2n-1} < u + v\sqrt{d} < \left(u_1 + v_1\sqrt{d}\right)^{2n+1}$$

et on peut écrire

$$u_n + v_n\sqrt{d} < u + v\sqrt{d} < \left(u_n + v_n\sqrt{d}\right)\left(u_1 + v_1\sqrt{d}\right)^2 \tag{2.17}$$

et on a

$$\frac{1}{u_n + v_n\sqrt{d}} = -\left(u_n - v_n\sqrt{d}\right)$$

Avec $u_n + v_n\sqrt{d} > 0$ alors $\left(-u_n - v_n\sqrt{d}\right)$ est strictement positif, et en multipliant (2.17) par $-\left(u_n - v_n\sqrt{d}\right)$ on obtient

$$1 < -\left(u + v\sqrt{d}\right)\left(u_n - v_n\sqrt{d}\right) < \left(u_1 + v_1\sqrt{d}\right)^2 \tag{2.18}$$

On pose

$$\begin{aligned} a + b\sqrt{d} &= -\left(u + v\sqrt{d}\right)\left(u_n - v_n\sqrt{d}\right) \\ &= (dvv_n - uu_n) + \sqrt{d}uv_n - vu_n \end{aligned}$$

ce qui donne

$$\begin{aligned} a^2 - db^2 &= (dvv_n - uv_n)^2 - d\,(uv_n - vu_n)^2 \\ &= \left(u^2 - dv^2\right)\left(u_n^2 - dv_n^2\right) = (-1) \times (-1) = 1. \end{aligned}$$

Donc $a + b\sqrt{d}$ est solution de l'équation de Pell $x^2 - dy^2 = 1$, et comme $x_1 + y_1\sqrt{d}$ est la solution fondamentale de cette équation, alors d'après la première propriété on a

$$x_1 + y_1\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^2.$$

Alors l'inégalité (2.18) devient

$$1 < a + b\sqrt{d} < x_1 + y_1\sqrt{d}$$

ce qui est impossible selon la définition de $x_1 + y_1\sqrt{d}$, et on a

$$u + v\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^2.$$

Inversement, tous les entiers $u_n + v_n\sqrt{d}$ donnés par la formule

$$u_n + v_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^{2n-1}, \ n \in \mathbb{N}^*$$

sont aussi solutions de l'équation $x^2 - dy^2 = -1$ et on a

$$\begin{aligned}
-1 &= \left(u_1^2 - dv_1^2\right)^{2n-1} \\
&= \left[\left(u_1 + v_1\sqrt{d}\right)\left(u_1 - v_1\sqrt{d}\right)\right]^{2n-1} \\
&= \left(u_1 + v_1\sqrt{d}\right)^{2n-1}\left(u_1 - v_1\sqrt{d}\right)^{2n-1} \\
&= \left(u_1 + v_1\sqrt{d}\right)^{2n-1}\left[\left(u_1 + v_1\sqrt{d}\right)^{2n-1}\right]^{-1} \\
&= \left(u_n + v_n\sqrt{d}\right)\left(u_n + v_n\sqrt{d}\right)^{-1} \\
&= \left(u_n + v_n\sqrt{d}\right)\left(u_n - v_n\sqrt{d}\right) \\
&= u_n^2 - dv_n^2
\end{aligned}$$

ce qui montre que $u_n + v_n\sqrt{d}$ est solution de l'équation de $x^2 - dy^2 = -1$.

3. Toutes les solutions entières positives de l'équation $x^2 - dy^2 = 1$ sont données par $x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n$.

   De la propriété 1, on a $x_1 + y_1\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^2$ et

$$x_n + y_n\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^{2n}, \ n \in \mathbb{N}^*.$$

□

Exemple 2.2. Toutes les solutions entières positives de l'équation $x^2 - 13y^2 = -1$ sont données par

$$x_n + y_n\sqrt{13} = \left(18 + 5\sqrt{13}\right)^{2n-1},\ n = 1, 2 \ldots.$$

tel que $18 + 5\sqrt{13}$ est la solution fondamentale de l'équation $x^2 - 13y^2 = -1$. Et toutes les solutions entières positives de l'équation $x^2 - 13y^2 = 1$ sont données par

$$x_n + y_n\sqrt{13} = \left(18 + 5\sqrt{13}\right)^{2n},\ n = 1, 2 \ldots..$$

Théorème 2.5. *L'équation*

$$x^2 - dy^2 = -1 \tag{2.19}$$

où $d \equiv 1(mod\ 4)$ ou $d \equiv 2(mod\ 4)$, possède des solutions si est seulement si $x_1 \equiv 1(mod\ 2d)$ où $x_1 + y_1\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$.

Démonstration. les cas $d \equiv 0, 3(mod4)$ ont été exclus du théorème précédent parce que d'après la Proposition 2.2 l'équation (2.19) n'admet pas de solution.

Supposons que l'équation (2.19) admet des solutions, et notons sa solution fondamentale par $u_1+v_1\sqrt{d}$, alors

$$x_1 + y_1\sqrt{d} = \left(u_1 + v_1\sqrt{d}\right)^2$$

ce qui entraine

$$\begin{cases} x_1 = u_1^2 + dv_1^2 \\ y_1 = 2u_1v_1 \end{cases}$$

avec $u_1^2 = dv_1^2 - 1$, et par suite on a

$$x_1 = 2dv_1^2 - 1 \equiv -1 \,(\text{mod } 2d)\,.$$

Inversement, supposons que $x_1 + y_1\sqrt{d}$ soit la solution fondamentale de l'équation $x^2 - dy^2 = 1$ qui vérifie $x \equiv -1 \,(\text{mod } 2d)$, alors

$$x_1 = 2dk - 1,\ k \in \mathbb{N}.$$

En remplaçant la valeur de x_1 dans l'équation $x^2 - dy^2 = +1$, on obtient

$$(2dk - 1)^2 - dy_1^2 = 1$$

ce qui entraine

$$4k\,(dk-1)=y_1^2.$$

Ce qui donne forcément y_1 pair et il existerait $\delta \in \mathbb{N}^*$ tel que $y_1 = 2\delta$. Ce qui nous permet d'écrire $k(dk-1)=\delta^2$, et Comme $\operatorname{p\,gcd}(k, dk-1)=1$, alors k et $dk-1$ sont nécessairement des carrés. Par suite,

$$\exists m, n \in \mathbb{N}^* \text{ tel que } k=m^2 \text{ et } dk-1=n^2$$

et ainsi, on aura

$$m^2d-1=n^2$$

ce qui montre que $(n+m\sqrt{d})$ est solution de l'équation $x^2-dy^2=1$. □

2.3 Période de $\sqrt{d}$ et solutions fondamentales des équations de Pell $x^2 - dy^2 = \pm 1$

Soit l'équation de Pell-Fermat suivante $x^2-dy^2=1$, où d un entier positif non carré parfait, et soit $\alpha = x_1 + y_1\sqrt{d}$ sa solution fondamentale avec $\alpha^n = x_n + y_n\sqrt{d}$ une suite de solution de l'équation $x^2-dy^2=1$. Alors

$$x_n^2 = 1 + dy_n^2$$

ce qui implique que $\mathrm{x}_n^2 > dy_n^2$ et donc $x_n > y_n\sqrt{d}$.

D'autre part

$$x_n^2 - dy_n^2 = \left(x_n - y_n\sqrt{d}\right)\left(x_n + y_n\sqrt{d}\right)$$

alors

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

et ainsi, on a

$$\begin{aligned}\left|\frac{x_n}{y_n} - \sqrt{d}\right| &= \left|\frac{1}{y_n\left(x_n + y_n\sqrt{d}\right)}\right| \\ &< \frac{1}{y_n^2 + y_n^2\sqrt{d}y_n} \\ &< \frac{1}{2y_n^2}, \text{ puisque } y_n \geq 1\end{aligned}$$

D'après le Théorème (1.6), $\dfrac{x_n}{y_n}$ est une réduite de la fraction continue qui représente $\sqrt{d}$ et on en déduit que le développement en fractions continues de $\sqrt{d}$ nous fournis la solution fondamentale en terme de réduite.

Ainsi, le développement en fractions continues de $\sqrt{d}$ permet de dire si l'équation $x^2 - dy^2 = -1$ possède des solutions ou non en fonction de sa longueur, comme le montre le théorème suivant :

Théorème 2.6. *[29]*

Soit ℓ la période du développement en fraction continue de $\sqrt{d} = [a_0; \overline{a_1, ...a_{\ell-1}, 2a_0}]$.

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

Exemple 2.3. .

1. soit l'équation $x^2 - 17y^2 = \pm 1$, et $\sqrt{17} = [4; \overline{8}]$, la période étant $\ell = 1$, étant impair ; alors l'équation $x^2 - 17y^2 = -1$ admet pour solution fondamentale le nombre $\alpha = p_0 + q_0\sqrt{17}$ où $\dfrac{p_0}{q_0} = [4] = \dfrac{4}{1}$ ce qui donne $\alpha = 4 + \sqrt{17}$ et la solution fondamentale de $x^2 - 17y^2 = 1$ est $\left(4 + \sqrt{17}\right)^2 = 33 + 8\sqrt{17}$.
2. Soit l'équation $x^2 - 11y^2 = \pm 1$ avec $\sqrt{11} = [3; \overline{3, 6}]$ et la période étant $l = 2$ pair. Alors l'équation $x^2 - 11y^2 = -1$ n'admet pas de solution et la solution fondamentale de l'équation $x^2 - 11y^2 = 1$ est $\alpha = p_1 + q_1\sqrt{11}$ où $\dfrac{p_1}{q_1} = [3; 3] = \dfrac{a_1a_0 + 1}{a_1} = \dfrac{10}{3}$ et donc $\alpha = 10 + 3\sqrt{11}$.
   Une autre méthode consiste à poser que $x_1 + y_1\sqrt{11}$ est la solution fondamentale de l'équation $x^2 - 11y^2 = 1$ avec y_1 soit le plus petit entier naturel non nul tel que $1 + 11y_1^2$ soit un carré parfait, ce qui donne $y_1 = 3$ et donc $x_1 = 10$.

Les solutions $x + y\sqrt{d}$ de l'équation de Pell $x^2 - dy^2 = 1$ et de l'équation $x^2 - dy^2 = -1$ s'appellent les unités ou les inversibles de $\mathbb{Z}\left[\sqrt{d}\right]$.

les algorithmes les plus connus et pratiqués , ainsi que les plus efficaces utilisés pour le calcul de la solution fondamental sont :

— L'algorithme de Lenstra (voir [18] et [19])

— L'algorithme de Lagarias (voir [16])

— L'algorithme LMM (Lagrange-Mathew-Molin : cet algorithme était déjà connu par Lagrange (voir [23] et [24]) .

2.4 L'équation de Pell $x^2 - dy^2 = c$

Trouver les solutions de l'équation $x^2 - dy^2 = C$ dans $\mathbb{Z}$, revient à trouver les éléments α dans $\mathbb{Z}\left[\sqrt{d}\right]$ tel que $N(\alpha) = C$, où N désigne l'application norme. Cette application peut aussi ne pas avoir de solutions, mais si elle en a une, elle en a une infinité. La proposition suivante va nous permettre de relier les solutions de l'équation $x^2 - dy^2 = C$, $C \neq 1$ et celles de l'équation $x^2 - dy^2 = 1$.

Proposition 2.3. *Si $u + v\sqrt{d}$ est solution de l'équation $x^2 - dy^2 = C$ et que $X + Y\sqrt{d}$ est solution de l'équation $x^2 - dy^2 = 1$, alors*

$$\left(X + Y\sqrt{d}\right)\left(u + v\sqrt{d}\right) = (Xu + Yvd) + (Xv + Yu)\sqrt{d}$$

est une solution de l'équation $x^2 - dy^2 = C$.

Démonstration. Comme

$$(Xu + Yvd)^2 - d(Xv + Yu)^2 = (u^2 - dv^2)(X^2 - dY^2) = C$$

Alors $(X + Y\sqrt{d})(u + v\sqrt{d})$ est une solution de l'équation $x^2 - dy^2 = C$, d'où le résultat. □

Sur l'ensemble de solutions de l'équation $x^2 - dy^2 = C$, on définit la relation d'équivalence suivante :

$$\left(u_1 + v_1\sqrt{d}\right) \sim \left(u_2 + v_2\sqrt{d}\right) \Longleftrightarrow (u_2 + v_2\sqrt{d}) = (u_1 + v_1\sqrt{d})(X + Y\sqrt{d}$$

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

Proposition 2.4. *Deux solutions $(u_1 + v_1\sqrt{d})$ et $u_2 + v_2\sqrt{d})$ de l'équation $x^2 - dy^2 = C$ sont associées si et seulement si $u_1u_2 - dv_1v_2$ et $u_2v_1 - u_1v_2$ sont des multiples de C .*

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

$$u_2 + v_2\sqrt{d} = (u_1 + v_1\sqrt{d})(X + Y\sqrt{d})$$

alors

$$\begin{cases} u_2 &= Xu_1 + dYv_1 \\ v_2 &= Xv_1 + Yu_1 \end{cases}$$

ce qui donne

$$\begin{cases} u_2u_1 & = Xu_1^2 + dYv_1u_1 \\ dv_2v_1 & = dXv_1^2 + dYu_1v_1 \end{cases}$$

Alors $(u_1 + v_1\sqrt{d})$ et $(u_2 + v_2\sqrt{d})$ deux solutions de l'équation $x^2 - dy^2 = C$, et soit $X + Y\sqrt{d}$ une solution de $x^2 - dy^2 = 1$, de plus

$$u_2u_1 - dv_1v_2 = X(u_1^2 - dv_1^2) = XC.$$

D'autre part

$$\begin{cases} v_1u_2 & = Xu_1v_1 + dYv_1^2 \\ u_1v_2 & = Xu_1v_1 + Yu_1^2 \end{cases}$$

alors

$$v_1u_2 - u_1v_2 = -Y(u_1^2 - dv_1^2) = -YC.$$

Réciproquement, supposons qu'il existe X, Y dans $\mathbb{Z}$, vérifiant :

$$\begin{cases} u_2u_1 - dv_1v_2 & = XC \\ v_1u_2 - u_1v_2 & = YC \end{cases}$$

alors

$$\frac{u_2u_1 - dv_1v_2}{C} = X \text{ et } \frac{v_1u_2 - u_1v_2}{C} = Y$$

tels que

$$\left(\frac{u_2u_1 - dv_1v_2}{C}\right)^2 - d\left(\frac{v_1u_2 - u_1v_2}{C}\right)^2 = 1$$

avec

$$u_1 + v_1\sqrt{d} = (X + Y\sqrt{d})(u_2 + v_2\sqrt{d})$$

Ce qui prouve que les solutions $(u_1 + v_1\sqrt{d})$ et $(u_2 + v_2\sqrt{d})$ sont associées. □

Définition 2.2. Si K est une classe de solutions de l'équation $x^2 - dy^2 = C$, alors l'ensemble $\overline{K} = \left\{u - v\sqrt{d} \text{ où } u + v\sqrt{d} \in K\right\}$ est aussi une classe de solutions de la même équation appelée classe conjuguée de la classe K.

Si $K = \overline{K}$, on dit que la classe est ambige. Dans une classe K non ambige, il existe une seule solution $\left(u^* + v^*\sqrt{d}\right)$ avec v^* positif minimal, $-u^* + v^*\sqrt{d} = -(u^* - v^*\sqrt{d}$ étant dans $\overline{K}$, appelée solution fondamentale de la classe K, et $-u^* + v^*\sqrt{d}$ est la solution fondamentale de la classe conjuguée $\overline{K}$. De même dans une classe ambige K, il existe une seule solution $u^* + v^*\sqrt{d}$, avec v^* positif minimal et

$u^* \geq 0$, et cette solution est dite solution fondamentale de classe K.

Si $u+v\sqrt{d}$ est une solution positif de l'équation $x^2-dy^2=C$, alors $u+v\sqrt{d}$ est dans une certaine classe de solutions K, et il existe $m \in \mathbb{N}$ tels que

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

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

Les deux lemmes suivants, dus à Nagel [25] , sont fondamentaux dans l'étude des équations de Pell ; ils nous seront utiles pour les preuves des théorèmes...

Lemme 2.1. *Si $u+v\sqrt{d}$ est la solution fondamentale d'une classe K de solutions de l'équation $x^2-dy^2=C$ tel que $C>0$, et $x_1+y_1\sqrt{d}$ est la solution fondamentale de l'équation $x^2-dy^2=1$, alors*

$$0 \leq |u| \leq \sqrt{\frac{(x_1+1)\,C}{2}} \tag{2.20}$$

et

$$0 < v \leq y_1\sqrt{\frac{C}{2\,(x_1+1)}} \tag{2.21}$$

Démonstration. On a vu que si K désigne une classe de solutions non ambige et $u+v\sqrt{d}$ est sa solution fondamentale, alors $-u+v\sqrt{d}$ est la solution fondamentale de la classe conjuguée $\overline{K}$. Ainsi, si les inégalités sont vraies pour une classe K, elles le sont pour la classe conjuguée $\overline{K}$.

On peut donc supposer $u>0$, et Comme $x_1+y_1\sqrt{d}$ est la solution fondamentale de l'équation $x^2-dy^2=1$, et $u+v\sqrt{d}$ est la solution fondamentale de l'équation $x^2-dy^2=C$, alors

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

ce qui, par multiplication, donne

$$\left(u^2-C\right)\left(x_1^2-1\right)=d^2v^2y_1^2.$$

Sachant que $\left(u+v\sqrt{d}\right)\left(x_1-y_1\sqrt{d}\right)=(ux_1-dvy_1)+(x_1v-y_1u)\sqrt{d}$ est une solution associée à la solution $u+v\sqrt{d}$, alors elle est dans la même classe que $u+v\sqrt{d}$ qui est la solution fondamentale de la classe K, d'où

$$u \leq ux_1-dvy_1$$

ce qui s'écrit

$$0 < dvy_1 \leq (x_1 - 1)\, u$$

et en passant aux carrés on aura

$$d^2v^2y_1^2 \leq (x_1 - 1)^2\, u^2$$

et comme on a $\left(u^2 - C\right)\left(x_1^2 - 1\right) = d^2v^2y_1^2$, alors

$$\left(u^2 - C\right)\left(x_1^2 - 1\right) \leq (x_1 - 1)^2\, u^2$$

ce qui donne

$$u^2 - C \leq \frac{(x_1 - 1)^2\, u^2}{\left(x_1^2 - 1\right)} = \frac{(x_1 - 1)}{(x_1 + 1)} u^2$$

et l'on obtient

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

que l'on peut écrire

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

et par conséquent, on aura

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

La deuxième inégalité s'obtient en observant que $u^2 = dv^2 + C$, ce qui permet d'écrire

$$dv^2 + C \leq \frac{(x_1 + 1)\, C}{2}$$

ce qui entraine

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

et donc

$$0 < v^2 \leq \frac{(x_1 - 1)\, Cy_1^2}{2dy_1^2}$$

ce qui entraine, sachant que $dy_1^2 = x_1^2 - 1$,

$$0 < v^2 < \frac{(x_1 - 1)\, Cy_1^2}{2\left(x_1^2 - 1\right)}$$

et par conséquent, on a

$$0 < v^2 \leq \frac{Cy_1^2}{2\,(x_1 + 1)}$$

d'où la relation

$$0 < v \leq \sqrt{\frac{C}{2\left(x_1+1\right)}} y_1$$

ce qu'il fallait démontrer. □

Exemple 2.4. La solution fondamentale de l'équation $x^2 - 11y^2 = 1$ étant $10+3\sqrt{11}$. On cherche les solutions $u+v\sqrt{d}$ avec $0 < |u| < \sqrt{\frac{(10+1)\,5}{2}}$ (d'après le lemme précédent), d'où l'équation $x^2-11y^2 = 5$ possède exactement deux classes de solutions : la classe de $4+1\sqrt{11}$ et sa classe conjuguée qui et la classe de $-4+1\sqrt{11}$.

Lemme 2.2. *Si $u+v\sqrt{d}$ est la solution fondamentale d'une classe de solutions K de l'équation $x^2 - dy^2 = -C$ et $x_1 + y_1\sqrt{d}$ est la solution fondamentale de l'équation $x^2 - dy^2 = 1$, alors*

$$0 < |u| \leq \sqrt{\frac{(x_1-1)\,C}{2}} \tag{2.22}$$

et

$$0 \leq v \leq \frac{y_1}{\sqrt{2\left(x_1-1\right)}}\sqrt{C} \tag{2.23}$$

Démonstration. On a vu que si K désigne une classe de solutions non ambige de solution fondamentale $u+v\sqrt{d}$, alors $-u+v\sqrt{d}$ est la solution fondamentale de la classe conjuguée $\overline{K}$. Ainsi, si les inégalités précédentes sont vraies pour une classe K, alors elles le sont aussi pour la classe conjuguée $\overline{K}$, donc on peut supposer $u > 0$. Alors

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

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

$$v \leq x_1v - y_1u$$

et donc

$$y_1u \leq v\left(x_1-1\right)$$

ce qui donne

$$dy_1^2u^2 \leq dv^2\left(x_1-1\right)^2$$

et comme $u^2 = -C + dv^2$, on aura

$$dy_1^2 \left(-C + dv^2\right) \leq dv^2 \left(x_1 - 1\right)^2$$

Autrement dit, sachant que $dy_1^2 = x_1^2 - 1$, on a

$$\frac{x_1 + 1}{x_1 - 1} \left(dv^2 - C\right) \leq dv^2$$

dont il en résulte

$$\frac{x_1 + 1}{x_1 - 1} \leq \frac{dv^2}{dv^2 - C}$$

ce qui entraine

$$\frac{x_1 + 1}{x_1 - 1} \leq 1 + \frac{C}{dv^2 - C}.$$

De cette inégalité et du fait que $u^2 = vv^2 - C$, on aura

$$u^2 \leq \frac{C\left(x_1 - 1\right)}{2} \tag{2.24}$$

ce qui équivaut à

$$0 \leq |u| \leq \sqrt{\frac{C\left(x_1 - 1\right)}{2}}.$$

De l'inégalité (2.24) on obtient

$$dv^2 - C \leq \frac{C\left(x_1 - 1\right)}{2}$$

ce qui donne

$$dv^2 \leq \frac{C\left(x_1 + 1\right)}{2}$$

et ainsi, on obtient

$$v^2 \leq \frac{C\left(x_1 + 1\right)}{2d} . \frac{x_1 - 1}{x_1 - 1} = \frac{Cdy_1^2}{2d\left(x{-}1\right) - 1} = \frac{Cy_1^2}{2\left(x_1 - 1\right)}$$

et par suite

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

□

Les lemmes précédents donnent des bornes pour la recherche des solutions fondamentales. en ce sens que :

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

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

Exemple 2.5. .

1. Soit l'équation

$$x^2 - 3y^2 = 184$$

La solution fondamentale de l'équation $x^2 - 3y^2 = 1$ étant $2 + \sqrt{3}$ et les les solutions suivantes

$$14 + 2\sqrt{3} \text{ et } -14 + 2\sqrt{3}$$

de $x^2 - 3y^2 = 184$ satisfont les inégalités du Lemme 21. Alors, et d'après la proposition 2.4, ces nombres sont toutes les solutions fondamentales dans différentes classes. Ainsi le nombre de classe est deux.

Chapitre 3

Sur l'équation diophantiennes Quadratique $x^2 - kxy + ky^2 + ly = 0$

Dans cette section, nous étudions l'équation diophantienne $x^2 - kxy + ky^2 + ly = 0$ pour des entiers k et l avec k pair. Nous donnons une caractérisation des solutions positives de cette équation selon les valeurs des entiers k et l. Nous étudierons également cette équation lorsque $l = 3^n$ et $k \equiv 2(\text{mod } 3)$; $l = 2^r 3^s$ et $k = 2k^{'} + 1$ avec $k^{'} \equiv 2(\text{mod } 3)$ oùn, s, et t sont des entiers naturels.

Introduction

Il y a eu beaucoup de travaux sur le titre d'équation diophantienne et l'étude de cette équation est liée à la théorie des équations de Pell. Pour les entiers k et l, Hu et Le [12] ont étudié l'équation

$$x^2 - kxy + y^2 + lx = 0 \tag{3.1}$$

pour $l = 1$. Marlewski et Zarzycki [21] ont montré que cette équation a un nombre infini de solutions entières positives si et seulement si $k = 3$ et ils se ont posé la question de savoir s'il existe d'autre valeurs de k pour lesquelles l'équation (3.1) contient une infinité de solutions entières. Keskin [14] a traité l'équation (3.1) pour $l = -1$ et 1. Il a montré que pour $k > 3$, l'équation (3.1) avec $l = 1$ n'a pas de solution entière positive. Il a également considéré les équations diophantiennes $x^2 - kxy - y^2 \pm y = 0$ et il a prouvé que ces équations ont des solutions entières positives pour $k \geq 1$. Suite à cela, Yuan et Hu [30] ont répondu positivement à la question de Marlewski et Zarzycki [21] en prouvant que l'équation (3.1) pour $l = 1$, a une infinité de solutions entières si et seulement si $k \neq 0$ et $k \neq \pm 1$. Ils ont également considéré l'équation (3.1) pour$l = 2$ et $l = 4$ et ont déterminé pour quelles valeurs de l'entier positif k ces équations ont une infinité de solutions entières positives. Keskin, Siar et Karaatli [15] ont

traité l'équation $x^2-kxy+y^2+2^n=0$ et ont déterminé les conditions nécessaires pour qu'elle admette une infinité de solutions entières positives pour $0 \leq n \leq 10$.
Karaatli et Siar [13] ont considéré l'équation diophantienne

$$x^2-kxy+ky^2+ly=0 \tag{3.2}$$

pour $l=2^n$,$0 \leq n \leq 3$, et ont déterminé les valeurs de l'entier positif k pour lesquelles cette équations admet une infinité de solutions entières positives. Récemment, Mavecha [22] a considéré l'équation (3.2) pour $l=2^n$ où n est un entier non négatif et k un entier impair. Elle a prouvé que cette équation contient une infinité de solutions entières positives x et y si et seulement si $k=5$.
Dans ce chapitre, nous traitons l'équation (3.2) pour les entiers k et l, où k est pair, et nous déterminons les valeurs des entiers k et l pour qu'une telle équation contienne une infinité de solutions entières positives. Nous traitons dans le même sillage l'équation lorsque $l=3^n$ et $k \equiv 2(\bmod 3)$; $l=2^r3^s$ et $k=2k^{'}+1$ avec $k^{'} \equiv 2(\bmod 3)$ où n, s et t sont des entiers non-négative.

3.1 Equation de la forme $x^2-kxy+ky^2+ly=0$ pour $l=2^n$, $0 \leq n \leq 3$

Karaatli et Siar [13] ont considéré l'équation diophantienne

$$x^2-kxy+ky^2+ly=0 \tag{3.3}$$

pour $l=2^n$, $0 \leq n \leq 3$ et ont prouvé que l'équation (3.2) a un nombre infini de solutions entières positives x et y si et seulement si

$$(k,l) \in \{(5,1)(5,2)(6,2)(5,4)(6,4)(8,4)(5,8)(6,8)(8,8)\}.$$

Nous aurons besoin pour cela des résultats de deux Lemmes ci-dessous, qui seront très utile dans la démonstration des théorèmes principaux, puis nous donnerons les preuves des principaux théorèmes de Karaatli et Siar.

Lemme 3.1. *[13] Pour $d>2$, on considère si $u_0+v_0\sqrt{d}$ est une solution fondamentale de l'équation $u^2-v^2d=\pm 2$. Alors $\dfrac{u_0^2+dv_0^2}{2}+u_0v_0\sqrt{d}$ est la solution fondamentale de l'équation $x^2-dy^2=1$.*

Lemme 3.2. *[13] L'équation $u^2-\left(k^2-4\right)^2=-4$ admet des solutions entières positives u et v si, et seulement si, $k=3$*

Karaatli et Siar on montré les résultats principaux suivants

Théorème 3.1. *L'équation*

$$x^2 - kxy + ky^2 + y = 0 \tag{3.4}$$

admet une infinité de solutions entières positives x et y si et seulement si $k = 5$.

Démonstration. Supposons qu'il existe existe des entiers positifs x et y tels que $x^2 - kxy + ky^2 + y = 0$.

Il s'ensuit que $y \mid x^2$, alors $\exists z \in \mathbb{N}$ tel que $x^2 = yz$. De plus, $\operatorname{p\,gcd}(y, z) = 1$. En effet, supposons pgcdd$(y, z) = c$, en remplaçant $y = cy'$ et $z = cz'$ dans l'équation $x^2 - kxy + ky^2 + y = 0$, on obtient -$cz' + k\sqrt{(c^2z'y')} - kcy' = 1$ ce qui implique que $c|1$. Par suite, $\exists a, b \in \mathbb{N}$ tels que $y = a^2$ et $z = b^2$ avec $pgcd(a, b) = 1$, ce qui entraine que $x = ab$. Substituons ses valeurs de x et y à l'équation (3.4) , on obtient

$$b^2 - kab + ka^2 + 1 = 0 \tag{3.5}$$

En multipliant l'identité par 4 nous obtenons

$$(4b^2 - 4kab - k^2a^2) + (k^2a^2 + 4ka^2) + 4 = 0$$

et donc

$$(2b - ka)^2 + ((k - 2)^2 - 4)a^2 = -4$$

ce qui, d'après le lemme3.2, donne $k - 2 = 3$, soit $k = 5$. □

Théorème 3.2. *l'équation*

$$x^2 - kxy + ky^2 + 2y = 0 \tag{3.6}$$

admet une infinité de solutions entières positives x et y si et seulement si $k = 5$ et 6.

Démonstration. Supposons que $x^2 - kxy + ky^2 + 2y = 0$ pour certains entiers positifs x et y, il s'en suit que $y \mid x^2$ et donc $\exists z \in \mathbb{N}$ tel que $x^2 = yz$. Soit $d = \text{pgcd}(y, z)$ alors $\exists a, b \in \mathbb{N}$ tels que $y = da^2$ et $z = db^2$ avec $\text{pgcd}(a, b) = 1$ et par suite $x = dab$.
En substituant ces valeurs de x et y dans l'équation(3.6). Nous obtenons

$$db^2 - kdab + kda^2 + 2 = 0 \tag{3.7}$$

ce qui implique que $d \mid 2$, soit donc $d \in \{1, 2\}$. Examinons séparément chacune des valeurs de d.

Cas 1. $d = 2$. Alors l'équation (3.7) devient l'équation (3.5) ce qui donne $k = 5$.

Cas 2. $d=1$. Dans ce cas, l'équation (3.7) devient

$$b^2-kab+ka^2=-2 \tag{3.8}$$

et par un calcul simple on montre que k est pair. En complétant l'expression (3.8) pour obtenir un facteur carré, on obtient

$$\left(b^2-kab+\frac{k^2}{4}a^2\right)-\left(\frac{k^2}{4}-k\right)a^2=-2$$

ce qui s'écrit

$$\left(b-\frac{k}{2}a\right)^2-\left(\left(\frac{k}{2}-1\right)^2-1\right)a^2=-2.$$

Posons $t=\dfrac{k}{2}-1$, l'équation précédente s'écrit

$$\left(b-\frac{k}{2}a\right)^2-\left(t^2-1\right)a^2=-2$$

et pour $u=b-\dfrac{k}{2}a$, considérons l'équation de Pell- généralisée

$$u^2-\left(t^2-1\right)a^2=-2. \tag{3.9}$$

dont la solution fondamentale est notée $u_0+v_0\sqrt{t^2-1}$.
Puisque$t^2-1=\dfrac{k^2}{4}-k>2$ pour $k>2$ et $t>1$, alors, par du Lemme 3.1, on a

$$\frac{u_0^2+(t^2-1)v_0^2}{2}+u_0v_0\sqrt{t^2-1}$$

est la solution fondamental de l'équation $x^2-(t^2-1)y^2=1$, pour $t>1$. Comme $(t,1)$ est la solution fondamentale de l'équation $x^2-(t^2-1)y^2=1$, alors, par le Théorème 2.1, nous obtenons

$$\begin{cases} \frac{u_0^2+(t^2-1)v_0^2}{2}=t \\ u_0v_0=1 \end{cases}$$

Ainsi, $u_0=v_0=1$ et $t^2-2t=0$, ce qui donne $t=2$ et donc $k=6$. Ce qui complète la preuve du théorème 3.2.

$\square$

Théorème 3.3. *l'équation*

$$x^2 - kxy + ky^2 + 4y = 0 \tag{3.10}$$

admet une infinité de solutions entières positives x et y si et seulement si $k = 5, 6,$ et 8.

Démonstration. Supposons que $x^2 - kxy + ky^2 + 4y = 0$ pour certains entiers positifs x et y. Il s'ensuit que $y \mid x^2$ alors $\exists z \in \mathbb{N}$ tel que $x^2 = zy$. Soit $d = \text{pgcd}(y, z)$, alors $\exists a, b \in \mathbb{N}$ tels que $y = da^2$ et $z = db^2$ avec $pgcd(a, b) = 1$. Il s'ensuit donc que $x = dab$.

En substituant ces valeurs de x et y à l'équation(3.10), nous obtenons

$$db^2 - kdab + kda^2 + 4 = 0 \tag{3.11}$$

ce qui implique que $d \mid 4$, et donc $d \in \{1, 2, 4\}$.

Cas 1. $pgcd(y, z) = d = 4$, alors $y = 4a^2$,$z = 4b^2$ et $x = 4ab$, avec pgcd $(a, b) = 1$. En substituant ces valeurs de x et y dans l'équation (3.10), on obtient l'équation(3.5) ce qui donne k=5.

Cas 2. $pgcd(y, z) = d = 2$. Alors $y = 2a^2$, $z = 2b^2$ et $x = 2ab$, avec pgcd$(a, b) = 1$. En substituant ces valeurs de x et dans l'équation (3.10), on obtient l'équation (3.8), ce qui implique que $k = 6$.

Cas 3. $pgcd(y, z) = d = 1$. Alors $y = a^2$, $z = b^2$ et $x = ab$, avec pgcd$(a, b) = 1$. En substituant ces valeurs de x et y dans l'équation (3.10), on obtient l'équation

$$b^2 - kab + ka^2 = -4 \tag{3.12}$$

ce qui donne nécessairement k pair, car sinon a et b doivent êtres pairs ce qui est impossible puisque pgcd$(a, b) = 1$. Par conséquent, b est pair et a impair, et donc il existe un entier positif c tel que $b = 2c$. Il s'ensuit que $4 \mid k$, ou encore $k = 4s$ pour un certain entier positif $s > 1$. En substituant ces valeurs de b et k dans l'équation (3.12), on obtient

$$c^2 - 2sca + sa^2 = -1$$

et donc

$$\left(c^2 - 2sca + s^2a^2\right) - \left(s^2a^2 - sa^2\right) = -1$$

et en d'autres termes

$$(c - sa)^2 - \left(s^2 - s\right) a^2 = -1 \tag{3.13}$$

Considérons alors l'équation

$$x^2-\left(s^2-s\right)y^2=-1 \tag{3.14}$$

où $s>1$, ce qui signifie que $\left(s^2-s\right)\geq 2$, et l'on obtient

$$\left(\sqrt{2}x\right)^2-2\left(s^2-s\right)y^2=-2 \tag{3.15}$$

sachant que $2\left(s^2-s\right)\geq 4$. En notant par $\sqrt{2}u_0+v_0\sqrt{2\left(s^2-s\right)}$ la solution fondamentale de l'équation $(3;15)$, alors, d'après le Lemme 3.1, on a

$$\frac{\left(\sqrt{2}u_0\right)^2-2\left(s^2-s\right)v_0^2}{2}+2u_0v_0\sqrt{s^2-s}=u_0^2+\left(s^2-s\right)v_0^2+2u_0v_0\sqrt{s^2-s}$$

est la solution fondamental de l'équation $x^2-\left(s^2-s\right)y^2=1$ pour $s>1$, et comme $(2s-1,2)$ est la solution fondamental de l'équation $x^2-\left(s^2-s\right)y=1$ alors par le Théorème (2.3), on obtient $u_0^2+(s^2-s)v_0^2=2s-1$ et $2u_0v_0=2.$, ce qui montre que $(u_0,v_0)=(1,1)$. Il s'ensuit que $s=1$ ou $s=2$. Sachant que $s>1$, alors $s=2$ et, par conséquent, entraine que $k=8$. Ce qui complète la preuve du théorème.

□

Théorème 3.4. *L'équation*

$$x^2-kxy+ky^2+8y=0 \tag{3.16}$$

possède une infinité de solutions entières positives x et y si et seulement si $k=5,6,8,$ et12.

Démonstration. Supposons que $x^2-kxy+ky^2+8y=0$ pour certains entiers positifs x et y, il s'ensuit que $y\mid x^2$ et on écrit $x^2=zy$ avec $z\in\mathbb{N}$.

Soit $d=\text{pgcd}(y,z)$, alors $\exists a,b\in\mathbb{N}$ tels que $y=da^2$, $z=db^2$, avec $\text{pgcd}(a,b)=1$, et on écrit $x=dab$.

En substituant ces valeurs de x et y dans l'équation (3.16), nous obtenons

$$db^2-kdab+kda^2+8=0 \tag{3.17}$$

ce qui implique que $d\mid 8$, en d'autres termes on $d\in\{1,2,4,8\}$.

Examinons dans ce qui suit chacune des valeurs de d

Cas 1. d=pgcd$(y,z)=8$. Alors $y=8a^2$, $z=8b^2$ et $x=8ab$, avecpgcd$(a,b)=1$. En remplaçant ces valeurs de x et y dans l'équation(3.17), on obtient l'équation (3.5) qui implique que $k=5$.

Cas 2. d=pgcd$(y,z)=4$, alors $y=4a^2$,$z=4b^2$ et $x=4ab$ avec pgcd$(a,b)=1$. En substituant ces valeurs de x et y dans l'équation(3.17), on obtient l'équation (3.8) ce qui implique que $k = 6$.

Cas 3. $d = \text{pgcd}(y, z) = 2$, alors $y = 2a^2$,$z = 2b^2$ et $x = 2ab$ avec $\text{pgcd}(a, b) = 1$. En substituant ces valeurs de x et y dans l'équation(3.17), on obtient l'équation (3.12) ce qui implique que $k = 8$.

Cas 4. d=pgcd$(y, z) = 1$, alors $y = a^2$, $z = b^2$ et $x = ab$ avec $\text{pgcd}(a, b) = 1$. En ces substituant ces valeurs de x et y dans l'équation(3.16), on obtient l'équation

$$b^2 - kab + ka^2 = -8. \tag{3.18}$$

Dans cette équation, on voit que si k est impair, alors les deux entiers a et b sont pairs, , ce qui est impossible puisque $\text{pgcd}(a, b) = 1$. Ainsi, k est un entier pair et nous en concluons que b est pair et donc il existe un entier positif c tel que $b = 2c$. De plus, comme $\text{pgcd}(a, b) = 1$, alors a est impair et donc $4|k$ et on écrit $k = 4s$ pour certains entiers positifs $s > 1$.
En substituant ces valeurs de b et k dans l'équation (3.18), on obtient

$$c^2 - 2sca + sa^2 = -2.$$

En complétant pour obtenir un carré dans le premier membre, on aura

$$(c - sa)^2 - \left(s^2 - s\right) a^2 = -2$$

qui est une équation de la forme

$$u^2 - \left(s^2 - s\right) v^2 = -2 \tag{3.19}$$

— Si s=2, on aura l'équation $u^2 - 2v^2 = -2$, qui admet une infinité de solutions et dont $4 + 3\sqrt{2}$ en est une, et ainsi, nous obtenons $k = 8$.

Supposons maintenant que $u_0 + v_0\sqrt{(s^2 - s)}$ est la solution fondamentale de l'équation (3.19) pour $s > 2$. Alors, et selon le Lemme 3.1, il s'ensuit que

$$\frac{u_0^2 + (s^2 - s)v_0^2}{2} + u_0v_0\sqrt{(s^2 - s)}$$

est la solution fondamentale de l'équation $x^2 - \left(s^2 - s\right) y^2 = 1$, Pour $s > 2$, et sachant que, par le Théorème 2.3, $(2s - 1, 2)$ est la solution fondamental de l'équation $x^2 - \left(s^2 - s\right) y^2 = 1$, on aura

$$\frac{u_0^2+(s^2-s)v_0^2}{2}=2s-1 \quad \text{et} \quad u_0v_0=2$$

Ce qui entraine $(u_0,v_0)=(2,1)$ avec s=3, puisque pour $(u_0,v_0)=(1,2)$ on a $s\notin\mathbb{N}$ et par conséquent on aura $k=12$.

□

3.2 Equation de la forme $x^2-kxy+ky^2+\ell y=0$, k un nombre impair et $\ell=2^n$, $n\in\mathbb{N}$.

Dans [22] , Mavecha a étudié l'équation (3.3) pour k un nombre impair et $\ell=2^n$, où n est un entier non négatif. Elle a montré le résultat suivant

Théorème 3.5. *Si k un nombre impair et $\ell=2^n$, n un entier non négatif, alors L'équation (3.3) a des solutions positives si et seulement si $k=5$ et toutes les solutions sont de la forme $(x,y)=(ab,a^2)$ avec $pgcd(a,b)=1$ et $(2b-5a)^2-5a^2=-4$.*

Afin de prouver ce théorème, nous aurons besoin des lemmes auxiliaires suivants :

Lemme 3.3. *L'équation (3.3) a une solution si est seulement si l'équation*

$$X^2-kXY+kY^2+LY=0 \tag{3.20}$$

possède des solution, pour un certain entier $L\mid\ell$ tel que $pgcd(Y,L)=1$.

Démonstration. Supposons que l'équation (3.3) admet une solution (x,y), on supposera que pgcd(y,l)≠1, alors il existe un entier premier p tel que $p\mid\ell$ et $p\mid y$, ce qui implique que $p\mid kxy-ky^2-\ell y$ et donc $p\mid x$.

On pose alors, $x=px$' ,$y=py$' et $\ell=p\ell'$, où x' , y' et l' sont des entiers, et il s'ensuit que

$$p^2x'^2-kp^2x'y'+kp^2y'^2+\ell p^2y'=0$$

et donc on a

$$x'^2-kx'y'+ky'^2+\ell y'=0$$

Si pgcd $(y',\ell')>1$, nous répétons le même processus jusqu'à ce que $pgcd(Y,L)=1$ et $X^2-kXY+kY^2+LY=0$ avec $L\mid\ell$.

Inversement, si l'équation (3.20) a une solution $(x,y)\in\mathbb{N}^2$, avec $L\mid\ell$, alors en posant $a=\frac{\ell}{L}$, $x=aX$ et $y=aY$, pour certains entiers x et y, on aura $x^2-kxy+ky^2+ly=0$. □

On peut alors sans perte de généralité, supposer que p$gcd(y,\ell)=1$ et on a

Lemme 3.4. *Si (x,y) est une solution de (3.3) avec pgcd$(y,l)=1$, alors y est un carré.*

Démonstration. Soit (x,y) une solution de l'équation (3.2), il suffit de prouver que

$$y=\prod_{\substack{t \text{ pair}\\ p \text{ premier}}} p^t.$$

Soit p un nombre premier tel que $p^t\,||\,y$, $p^t\mid x^2$. Si de plus t est un nombre impair alors

$$p^{\frac{t+1}{2}}\mid x$$

ce qui, par un simple calcul, permet de trouver que

$$p^{\frac{3t+1}{2}}\mid xy,\ p^{t+1}\mid y^2 \text{ et } p^{t+1}\mid x^2$$

ce qui entraine que $p^{t+1}\mid\ell y$. Comme $p\nmid\ell$, alors $p^{t+1}\mid y$ ce qui est absurde par hypothèse. Ainsi, t est un nombre pair. □

Revenons à la preuve du Théorème 3.5 :

Nous devons résoudre l'équation (3.3), où pgcd $(y,\ell)=1$ et $\ell=2^n$ avec $n\geq 0$. Alors, d'après le Lemme 3.4, y est un carré. Soit $y=a^2$, alors $a^2\mid x^2$, i.e. $a\mid x$. Soit alors $x=ab$, où a et $b\in\mathbb{N}$, alors l'équation (3.3) implique que

$$a^2b^2-ka^3b+ka^4+\ell a^2=0$$

ce qui, par conséquent, donne

$$b^2-kab+ka^2+\ell=0.$$

Pour résoudre cette équations, nous examinons deux cas

Cas 1. Si $\ell=2^n$,$n\neq 0$, et comme pgcd$(y,\ell)=1$, alors a est impair ce qui donne $ka^2+\ell$ est impair puisque k est impair. Ainsi, l'entier $b^2-kab=b(b-ka)$ est pair pour tout entier naturel b, et donc $\left(b^2-kab\right)+(ka^2+l)$ est impair ce qui entraine que l'équation (3.3) n'a pas de solution.

Cas 2. Si $\ell = 2^0 = 1$, et par multiplication par 4 des deux membres de l'équation précédente, nous obtenons l'équation

$$(2b-ka)^{\,2} - \left((k-2)^{\,2}-4\right)a^2 = -4$$

qui est de la forme

$$u^2 - \left(\alpha^2-4\right)v^2 = -4.$$

Par le Lemme 3.2 , on déduit que $k=5$ et $(2b-5a)^2-5a^2=-4$, et en posant pgcd $(a,b)=c$ on tire que $c \mid \left(-b^2+kab-ka^2\right)=1$ ce qui entraine $c=1$.

D'après le théorème principal 3.5, nous savons que l'équation (3.3) a des solutions entières positives lorsque $\ell = 2^n$ et pour l'entier non négatif n et un entier impair k, si et seulement si $k=5$. Les solutions (x,y) sont obtenues à partir des solutions de l'équation de Pell généralisée

$$u^2-5v^2=-4$$

qui est connue pour avoir une infinité de solutions (u,v).

3.3 Equation de la forme $x^2-kxy+ky^2+\ell y=0$, pour $\ell=2^n$, $n\in\mathbb{N}$, et k un nombre pair, $\ell=3^n$, $n\in\mathbb{N}$ et $k\equiv 2 (\mathrm{mod}\ 3)$ et $\ell=2^r3^s$, $r,s\in\mathbb{N}$ et $k=2k^{'}+1$ avec $k'\equiv 2(\mathrm{mod}\ 3)$.

Une généralisation des résultats de Karaatli et Siar [13] d'un côté, et celui de Mavecha [22] de l'autre, nous donnons le théorème principal suivant ainsi quelques résultats associés.

Théorème 3.6. *Soient ℓ and k des entiers, avec k pair. Si $\ell^2<k$, alors l'équation*

$$x^2-kxy+ky^2+ly=0 \tag{3.21}$$

possède une infinité de solutions entière positives x et y si et seulement si $(l,k)=(2,6)$. De plus les solutions sont données par

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

où n est impair, u_n et v_n son donnés par

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

Démonstration. Supposons qu'il existe certains entiers x et y qui satisfont l'équation (3.21). En complétant le carré nous obtenons

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

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

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

Soient $u=2ay+\ell$ et $v=2x-ky$, nous obtenons l'équation

$$u^2-\left(\frac{k^2}{4}-k\right)v^2=\ell^2. \tag{3.22}$$

Dans l'équation (3.22), si $k=2$ nous obtenons l'équation $u^2+v^2=\ell^2$ qui a une infinité de solutions suivant les valeurs de ℓ.

Si $k=4$, nous obtenons alors $u^2=\ell^2$, et dans ce cas on a également une infinité de solutions. Par conséquent, nous pouvons supposer $k>4$ ce qui, en d'autres termes, veut dire que $\left(\dfrac{k^2}{4}-k\right)>0$ et donc l'équation (3.22) est une équation de Pell. La solution fondamentale de cette équation de Pell

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

est donnée par $u_1=\dfrac{k}{2}-1$ et $v_1=1$. De l'inégalité (2.21) du Lemme 2.1, nous aurons

$$0\le v^*\le \frac{v_1}{\sqrt{2\,(u_1+1)}}\sqrt{\ell^2}<\frac{\sqrt{k}}{\sqrt{k}}=1$$

Alors il n'ya qu'une seul classe de solutions et la solution fondamental de cette classe est donné par $v=0$ et $u=\pm\ell$. Les solutions infiniment nombreuses de cette classe peuvent être trouvées à partir de la formule

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

Alors u_n et v_n sont

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

Les solutions (x_n, y_n) de l'équation (3.21) 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 $k > 4$ (i.e.$k \geq 6$), et nous aurons $2\left(\frac{k^2}{4}-k\right) > k > l^2$ et comme $y_n \geq 1$, puisqu'on s'intéresse aux solutions entières positives, alors$u_n < 0$. Donc dans la suite, nous considérons que u_n est négatif. En prenant les équations modulo $(\frac{k}{2}-2)$, on obtient $u_n \equiv -\ell \pmod{\frac{k}{2}-2}$ et $u_n \equiv \ell \pmod{\frac{k}{2}-2}$. En d'autres termes, nous aurons $2\ell \equiv 0(mod\frac{k}{2}-2)$. Ainsi, $k-4$ divise 4ℓ. Sachant que $\ell^2-4 < k-4 \leq 4\ell$, nous aurons $\ell^2-4\ell-4 < 0$, et donc $\ell \in \{1,\ 2,\ 3,\ 4\}$.

Par suite, , nous déterminons pour chaque valeurs de ℓ celle correspondantes, s'il y en a, de k, de sorte que l'équation (3.21) ait une infinité de solutions entières positives.

□

— *Si $\ell = 1$, d'après ce qui précède, nous avons 4 est un multiple de $k-4$ pour $k > 1$. Ainsi $k \in 5, 6, 8$ et comme on ne s'intéresse qu'aux valeurs paires de k, alors $k \in 6, 8$. Pour ces valeurs de k, il n y a pas de solution entière positive de notre équation, et en considérant quelques congruences appropriées, comme nous allons voir.*

  — *pour $k = 6$, , et d'après ce qui précède, nous aurons les équations suivantes*

$$u_n = -\left(2^n + \sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2i}2^{n-2i}3^i\right) \tag{3.23}$$

$$-6y_n + 1 = u_n \tag{3.24}$$

De (3.24) nous avons $u_n \equiv 1(mod\ 2)$, alors que de l'équation (3.23) nous avons

$$u_n \equiv 0\,(mod\ 2) \tag{3.25}$$

ce qui est absurde.

— *Pour $k=8$, nous obtenons les équations suivantes*

$$u_n = -\left(3^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} 3^{n-2i} 8^i\right) \tag{3.26}$$

$$-16y_n + 1 = u_n \tag{3.27}$$

En regardant l'équation (3.27) modulo 8 on a $u_n \equiv 1\ (mod\ 8)$. L'équation (3.26) 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.

— *Si $\ell = 2$, alors $k-4$ divise divise 8, donc $k \in \{5,\ 6,\ 8,\ 12\}$ et comme on est dans le cas k pair et $k > 4$, on aura $k \in \{6,\ 8,\ 12\}$*

— *Pour $k=6$, de ce qui précède on aura*

$$u_n = -2\left(2^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} 2^{n-2i} 3^i\right) \tag{3.28}$$

$$-6y_n + 2 = u_n. \tag{3.29}$$

En considérant (3.29) modulo 3, on obtient $u_n \equiv 2\,(mod\ 3)$.

De (3.28), pour n pair nous trouvons que $u_n \equiv -2\,(mod\ 3)$ ce qui est contradictoire.

De (3.29) nous voyons que y_n existe si et seulement si 3 divise $(u_n - 2)$, ce qui est en accord avec (3.28) puisque $u_n \equiv 2\,(mod\ 3)$. En examinant le système suivant pour x_n

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

nous obtenons

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

Ainsi, x_n existe si et seulement si u_n et v_n ont la même parité, ce qui est vrai. Ainsi dans ce cas *nous avons une infinité de solutions entières positives et ces solutions sont données par*

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

— *Pour* $k = 8$, *on obtient les équations suivantes*

$$u_n = -2\left(3^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} 3^{n-2i} 8^i\right) \tag{3.30}$$

$$-16y_n + 2 = u_n. \tag{3.31}$$

L'équation (3.31) donne $u_n \equiv 2 \ (mod\ 8)$ *et* $u_n \equiv 2 \ (mod\ 16)$, *tandis que l'équation (3.30) donne*

$$u_n \equiv -2.3^n \, (mod\ 8) \equiv \begin{cases} -2 \, (mod\ 8) & si\ n\ est\ pair \\ -6 \, (mod\ 8) & si\ n\ est\ impair \end{cases}$$

ce qui est une contradiction.

— *Pour* $k = 12$, *on a les équations suivantes*

$$u_n = -2\left(5^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} 5^{n-2i} 24^i\right) \tag{3.32}$$

$$-48y_n + 2 = u_n \tag{3.33}$$

Dans(3.33), nous obtenons $u_n = 2 \, (mod\ 24)$, *tandis que dans l'équation (3.32) nous obtenons*

$$u_n \equiv -2.5^n \, (mod\ 24) \equiv \begin{cases} -2 \, (mod\ 24) & si\ n\ est\ pair \\ -10 \, (mod\ 24) & si\ n\ est\ impair \end{cases}$$

ce qui est une contradiction.

— *Si* $\ell = 3$, *alors 12 est un multiple de* $k - 4$, *et donc* $k \in \{5, 6, 7, 8, 10, 16\}$, *et comme on est dans le cas* k *pair et* $k > 9$, *nous allons donc vérifier les valeurs qui sont dans l'ensemble suivant* $k \in \{10, 16\}$

— *Pour $k=10$, on obtient les équations suivantes*

$$u_n=-3\left(4^n+\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2i}4^{n-2i}15^i\right) \tag{3.34}$$

$$-30y_n+3=u_n. \tag{3.35}$$

Dans l'équation (3.35) , nous obtenons $u_n\equiv 3\,(mod\ 30)$, tandis que dans l'équation (3.34) nous obtenons

$$u_n\equiv -3.4^n\,(mod\ 30)\equiv\begin{cases}-18\,(mod\ 30) & si\ n\ est\ pair\\ -12\,(mod\ 30) & si\ n\ est\ impair\end{cases}$$

ce qui est aussi une contradiction.

— *Pour $k=16$, nous avons les équations*

$$u_n=-3\left(7^n+\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2i}7^{n-2i}.48^i\right) \tag{3.36}$$

$$-96y_n+3=u_n. \tag{3.37}$$

En prenant l'équation (3.37) modulo48 on obtient $u_n\equiv 3\,(mod\ 48)$, mais dans l'équation (3.36) on obtient

$$u_n\equiv -3.7^n\,(mod\ 48)\equiv\begin{cases}-3\,(mod\ 48) & si\ n\ est\ pair\\ -21\,(mod\ 48) & si\ n\ est\ impair\end{cases}$$

ce qui est absurde.

— *Si l=4 , alors 16 est un multiple de $k-4$, et donc $k\in\{5,6,8,12,20\}$, et comme nous sommes intéressés par le cas k pair et $k>16$ ceci donne $k=20$. Dans ce cas, on a les équations suivantes*

$$u_n=-4\left(9^n+\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2i}9^{n-2i}.80^i\right) \tag{3.38}$$

$$-160y_n+4=u_n. \tag{3.39}$$

En considérant l'équation (3.39) modulo 80, on obtient $u_n\equiv 4\,(mod\ 80)$, et de l'équation

(3.38) nous obtenons

$$u_n \equiv -4.9^n \,(mod\ 80) \equiv \begin{cases} -4\,(mod\ 80) & si\ n\ est\ pair \\ -36\,(mod\ 80) & si\ n\ est\ impair \end{cases}$$

ce qui constitue une contradiction.

Nous déduirons dans les corollaires suivants les résultats de Karaatli et Siar [13] : Theorem 3.1, Theorem 3.2 et Theorem 3.3 et nous en donnons plus de précisions

Corollaire 3.1. .

1. *L'équation* $x^2 - kxy + ky^2 + y = 0$ *a une infinité de solutions entières positives* x *et* y *si et seulement si* $k = 5$.
2. *L'équation* $x^2 - kxy + ky^2 + 2y = 0$ *a une infinité de solutions entières positives* x *et* y *si et seulement si* $k = 5, 6$.
3. *L'équation* $x^2 - kxy + ky^2 + 4y = 0$ *a une infinité de solutions entières positives* x *et* y *si et seulement si* $k = 5, 6, 8$.

Démonstration. examinons les 3 cas séparément.

1. Mavecha a prouvé que la seule valeur de k impair pour laquelle il y a une infinité de solutions entières positives x et y est $k = 5$. Au vu du théorème précédent, il reste à considérer le cas k pair et $k \leq l^2 = 1$, et il n'y en a pas.
2. Le cas k impair est fait par Mavecha. Nous avons prouvé que lorsque k est pair et$l^2 < k$, alors la seule valeur de k pour laquelle il existe une infinité de solutions entières positives est $k = 6$. Par suite, il ne reste à traiter que les cas $k \leq l^2 = 4$ et k pair. Mais ces valeurs de k ont été exclues avant d'énoncer notre théorème.
3. Comme ci-dessus, nous rappelons qu'il est prouvé par Mavecha que $k = 5$ est la seule valeur de k impair telle que l'équation (3.21) contient une infinité de solutions entières positives x et y . Au vu de notre théorème principal, il reste à considérer le cas k pair où $4 < k \leq l^2 = 16$. Nous allons donc traiter les valeurs suivantes de k : $k \in \{6, 8, 10, 12, 14, 16\}$.

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

$$u_n = -4\left(2^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} .2^{n-2i}.3^i\right) \tag{3.40}$$

$$-6y_n+4=u_n. \tag{3.41}$$

Nous avons de l'équation (3.41) que $u_n \equiv 1(mod3)$, et l'équation (3.40) donne

$$u_n \equiv -4.2^n \pmod 3 \equiv \begin{cases} -1 \pmod 3 & \text{si } n \text{ est pair} \\ 1 \pmod 3 & \text{si } n \text{ est impair} \end{cases}$$

Pour n pair on a une contradiction. Pour n impair, et de $u_n=-2(3y_n-2)$ on tire que y_n existe si et seulement si

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

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. 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 sont donné par

$$u_n=-4\left(3^n+\sum_{i=1}^{\lfloor\frac{n}{2}\rfloor}\binom{n}{2i}.3^{n-2i}.8^i\right) \tag{3.42}$$

$$-16y_n+4=u_n. \tag{3.43}$$

En considérant l'équation (3.43) modulo 16, on obtient $u_n \equiv 4 \pmod{16}$, mais dans l'équation (3.42) nous obtenons

$$u_n \equiv -4.3^n \pmod{16} \equiv \begin{cases} -4 \pmod{16} & \text{si } n \text{ est pair} \\ 4 \pmod{16} & \text{si } n \text{ est impair} \end{cases}$$

Pour n pair nous obtenons une contradiction. Pour n impair et pour que y_n existe, il est nécessaire et suffisant que $u_n-4 \equiv 0(\text{mod } 16)$ ce qui est vrai dans l'équation(3.42). En outre, à partir du système d'équation suivant

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

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

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

— Pour $k = 10$, nous obtenons les équations suivantes

$$u_n = -4 \left(4^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} .4^{n-2i}.15^i \right) \tag{3.44}$$

$$-30y_n + 4 = u_n. \tag{3.45}$$

En considérant l'équation (3.45) modulo 30, on obtient $u_n \equiv 4 \pmod{30}$, mais dans l'équation (3.44) nous obtenons

$$u_n \equiv -4.4^n \pmod{30} \equiv \begin{cases} -4 \pmod{30} & \text{si } n \text{ est pair} \\ -16 \pmod{30} & \text{si } n \text{ est impair} \end{cases}$$

ce qui est contradictoire.

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

$$u_n = -4 \left(5^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i} .5^{n-2i}.24^i \right) \tag{3.46}$$

$$-48y_n + 4 = u_n. \tag{3.47}$$

En prenant modulo 48 l'équation (3.47), nous obtenons $u_n \equiv 4 \pmod{48}$. D'autre part, nous obtenons de l'équation (3.46) que

$$u_n \equiv -4.5^n \pmod{48} \equiv \begin{cases} -4 \pmod{48} & \text{si } n \text{ est pair} \\ -20 \pmod{48} & \text{si } n \text{ est impair} \end{cases}$$

ce qui aboutit à une contradiction.

— Pour $k=14$, nous obtenons les équations suivantes

$$u_n = -4\left(6^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i}.6^{n-2i}.35^i\right) \tag{3.48}$$

$$-70y_n + 4 = u_n. \tag{3.49}$$

En prenant modulo 35 l'équation (3.49), nous obtenons $u_n \equiv 4 \pmod{35}$. D'autre part, nous obtenons de l'équation (3.48) que

$$u_n \equiv -4.6^n \pmod{35} \equiv \begin{cases} -4 \pmod{35} & \text{si } n \text{ est pair} \\ -24 \pmod{35} & \text{si } n \text{ est impair} \end{cases}$$

ce qui aboutit à une contradiction.

— Pour $k=16$, nous obtenons les équations suivantes

$$u_n = -4\left(7^n + \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2i}.7^{n-2i}.48^i\right) \tag{3.50}$$

$$-96y_n + 4 = u_n. \tag{3.51}$$

En prenant modulo 48 l'équation (3.51), nous obtenons $u_n \equiv 4 \pmod{48}$. D'autre part, nous obtenons de l'équation (3.50) que

$$u_n \equiv -4.7^n \pmod{48} \equiv \begin{cases} -4 \pmod{48} & \text{si } n \text{ est pair} \\ -28 \pmod{48} & \text{si } n \text{ est impair} \end{cases}$$

ce qui aboutit à une contradiction.

□

Ainsi, nous avons fini, et les seules valeurs de k pour lesquelles l'équation (3.21) a une infinité de solutions entières positives x et y sont $k = 5, 6, 8$.

Remarque 3.1. Nous n'avons pas traité le cas $\ell = 2^3 = 8$ dans le théorème 3.6. Ce cas correspond au théorème 3.4 dans Karaatli et Siar. Mais, on peut dire, qu'au vu du théorème précédent et de Mavecha, il reste à traiter le cas k pair où $k \leq 64$. Nous devons donc traiter 32 équations où ℓ, k sont connues. Toutes ces équations peuvent être traitées de la même manière, donc nous traitons le cas $l = 8$ et $k = 8$. Dans ce cas, notre équation est donné par

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

De ce qu'on a vu ci-dessus, nous obtenons l'équation de Pell générale suivante

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

La solution fondamentale de l'équation de Pell $u^2 - 8v^2 = 1$ est $(u_1, v_1) = (3, 1)$. Par le Lemme 2.1, nous avons trouvé que

$$0 \leq v \leq \frac{v_1}{\sqrt{2(u_1+1)}}\sqrt{\ell^2} = 2\sqrt{2}.$$

Par conséquent $v \in 0, 1, 2$, mais $v = 1$ ou 2 ne vérifient pas l'équation générale de Pell. Ainsi, il existe une classe ambigüe de solution donnée par $v = 0$, alors $u = \pm 8$. L'infinité de solutions de cette classe peuvent être trouvées à partir de la formule

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

Par la machinerie développée au cours de la démonstration du théorème principale 3.6 nous obtenons les équations suivantes

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

et

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

Notons que du dernier système u_n est négatif. En analysant ces deux systèmes, nous voyons que pour que y_n existe nous devons avoir que $u_n - 8 \equiv 0 \pmod{16}$, ce qui est vrai, et pour que x_n existe, à partir de $4x_n-8=2v_n-u_n$, nous devons avoir $u_n$et v_n pairs, ce qui est également vrai. Alors dans ce cas, nous avons une infinité de solutions entières positives x et $y$de l'équation (3.21) donnée par les suites suivantes

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

Ceci est en accord avec le théorème 3.4 dans Karaatli et Siar.

Remarque 3.2. Pour traiter le cas $\ell=2^4=16$ du théorème 3.6, il reste à traiter avec k pair et $k\leq 2^8$. Donc, pour chaque valeur de ℓ, nous avons une borne sur k et il y a un nombre fini d'équations à résoudre. Comme tout ce qui reste sont des calculs et que tous ces cas peuvent être traités comme dans la dernière remarque, nous les omettons.

Nous avons aussi traité l'équation (3.21) quand $\ell=3^n$ et $k\equiv 2 (\text{mod } 3)$, $\ell=2^r.3^s$ et $k=2k'+1$ avec $k'\equiv 2(\text{mod } 3)$ où n, s, t sont des entiers non-négatifs, et pour ces valeurs de k et ℓ nous obtenons les théorèmes suivants

Théorème 3.7. *L'équation*

$$x^2-kxy+ky^2+ly=0 \tag{3.52}$$

où $l=3^n$ et $k\equiv 2(mod\ 3)$ sont des entiers et n un entier non-négatif, a une infinité de solution entières positives x et y si et seulement si $k=5$.

Démonstration. Nous examinerons la preuve selon deux cas

1. Supposons d'abord que $n>0$. Soit x et y des solutions à l'équation(3.52), alors le Lemme 3.3 dans Mavecha nous permet de supposer que $\text{pgcd}(y,\ell)=1$. Dans ce cas, et d'après le Lemme 3.4 dans Mavecha, y est un carré. En posant $y=\alpha^2$, donc à partir de l'équation (3.52) nous obtenons $x=\alpha t$ avec $t\in\mathbb{N}$. Par conséquent, l'équation (3.52) devient

$$t^2-k\alpha t+k\alpha^2+3^n=0 \tag{3.53}$$

Nous considérons les points suivants

— Si $3\mid t$, et comme $\text{pgcd}(y,l)=\text{pgcd}(\alpha^2,3^n)=1$, en considérant l'équation (3.53) modulo 3, on obtient que $k\equiv 0(\text{mod } 3)$ ce qui contredit notre hypothèse que $k\equiv 2(\text{mod } 3)$.

— Si $3\nmid t$ et en considérant l'équation (3.53) modulo3, on obtient que $-k\alpha t\equiv 0(\text{mod } 3)$, nous obtenons à nouveau une contradiction puisque aucun de ces entiers n'est divisible par 3 .

2. Considérons maintenant le cas $n=0$. Dans ce cas, l'équation (3.21) devient

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

Mais cette dernière équation est traitée dans le théorème 3.1 de Karaatli et Siar et il y est prouvé qu'il a une infinité de solutions entières positives si et seulement si $k=5$.

□

Théorème 3.8. *L'équation*

$$x^2 - kxy + ky^2 + ly = 0 \tag{3.54}$$

où $\ell = 2^r.3^s$, $k = 2k^{'} + 1$, $k' \equiv 2(mod\ 3)$ sont des entiers, r et s sont des entiers non-négatif, a une infinité de solution entières positives x et y si et seulement si $k=5$.

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

1. Supposons d'abord que $r>0$ et $s>0$. Soit x et y des solutions de l'équation(3.21). Alors le Lemme 3.3 de Mavecha nous dit que nous pouvons supposer que $\mathrm{pgcd}(y,\ell)=1$. Dans ce cas, il est indiqué dans le Lemme 3.4 également dans Mavecha, que y est un carré. En posant $y=\alpha^2$, donc de l'équation (3.21) nous obtenons $x=\alpha t$ avec $t\in\mathbb{N}$. Par conséquent, l'équation (3.21) devient
$$t^2 - k\alpha t + k\alpha^2 + 2^r.3^s = 0 \tag{3.55}$$
Considérons pour cela les cas suivants :
   (a) Si $3 \mid t$, puisque $\mathrm{pgcd}(y,l) = \mathrm{pgcd}(\alpha^2, 2^r.3^s) = 1$, et en considérant l'équation (3.55) modulo 3, on obtient que $k \equiv 0(\mathrm{mod}\ 2)$ qui contredit notre hypothèse que $k' \equiv 2(mod 3)$.
   (b) Si $2 \mid t$, en considérant l'équation (3.55) modulo 2, on obtient $k\equiv 0(\mathrm{mod}\ 2)$,ce qui contredit le fait que $k = 2k^{'}+1$.
   (c) Si $3 \nmid t$, en prenant aussi l'équation (3.55) modulo 3, on obtient que $-k\alpha t \equiv 0(\mathrm{mod}\ \ 3)$, une contradiction puisque aucun de ces entiers n'est divisible par 3.
   (d) si $2 \nmid t$,nous obtenons la même conclusion.
2. Si $r=0$ et $s\neq 0$ nous obtenons le Théorème 3.7 ci-dessus, et si $s=0$ et $r\neq 0$ nous obtenons le Théorème 3.5 dans Mavecha. Il reste donc à traiter le cas $r=s=0$.Dans ce cas, on obtient aussi le Théorème 3.1 de Karaatli et Siar, où ils ont prouvé que l'équation (3.21) contient une infinités de solutions entières positives si et seulement si $k=5$.

□

Chapitre 4

SUR L'EQUATION DIOPHANTIENNE $h(a)x^2 + f(a) = g(a)a^n$

Dans cette section, nous prouvons que l'équation intitulée n'a qu'un nombre fini de solutions, généralisant le travail de Li et Yuan [20] et un autre travail de Mua Hua-Le [11] Le. Nous appliquons notre méthode pour l'étude de l'équation diophtantienne spécifique considérée par Mua Hua-Le [11] et obtenons toutes les solutions.

4.1 Courbes elliptiques

4.1.1 Introduction

L'étude des points à coordonnées rationnelles sur une courbe algébrique est liée à la recherche des solutions entières d'équations diophantiennes, des solutions qui sont à fortiori des solutions rationnelles. Une courbe algébrique est le lieu des zéros dans le plan d'un polynôme à deux variables. À toute courbe algébrique, on peut associer un entier positif, appelé le genre, que l'on peut exprimer comme $g= \frac{(d-1)(d-2)}{2}$, où d est le degré de la courbe. Le présent chapitre porte sur les courbes de genre 1 (de degré 3), les courbes elliptiques. Celles ci sont munies d'une loi de groupe abélien naturelle, qui facilite leur étude. La théorie des courbes elliptiques est riche, varié et étonnamment vaste. Elle a de nombreuses applications importantes dans des domaines très différents des mathématiques. Elles interviennent en théorie de nombres, en cryptologie dans le problème de la factorisation des entiers ou pour fabriquer des codes performants. . .etc.,

4.1.2 Définitions

Définition 4.1. [29]

une courbe elliptique E sur un corps K est une courbe non singulière projective du genre 1, avec un point K-rationnel O_E.

Une courbe elliptique est un objet abstrait et peut comporter de nombreux modèles, comme le modèle défini ci-dessous

Définition 4.2. [29]

(équation Weierstrass) Une équation de Weierstrass, dite projective, d'une courbe elliptique E sur un corps K est de la forme

$$\tilde{E} \,:\, y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{4.1}$$

où $a_1, a_2a_3, a_4, a_6 \in K$.

Elle est définie dans le plan projectif $\mathbb{P}^2(K)$ dont la version affine est de la forme

$$E \,:\, y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.2}$$

(4.2) est appelé équation généralisée de Weierstrass. Son discriminant est définit comme suit

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \neq 0$$

avec

$$b_2 = a_1^2 + 4a_2 \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

En opérant certains changements de variables, il est possible de simplifier l'écriture de courbes elliptiques.

Définition 4.3. [29] (Equation simplifier de Weierstrass)

Soit E_1 et E_2 deux courbes elliptiques définies sur K, alors E_1 et E_2 sont isomorphes sur K s'il existe u, r, s, $t \in K$, $u \neq 0$ avec le changement de variables suivant

$$(x, y) \longmapsto \left(u^2x + r, u^3y + u^2sx + t\right)$$

transformant l'équation de E_1 en E_2 . Avec un choix judicieux des paramètres u, r, s et t on peut obtenir une forme de l'equation de Weierstrass avec moins de paramètres. Pour les corps K de caractéristiques $\neq 2$ et 3, le changement de variables à opérer est :

$$\begin{array}{r} y \longmapsto \frac{1}{2}\left(y - a_1 x - a_3\right) \\ (x, y) \longmapsto \left(\dfrac{x - 3b_2}{36}, \dfrac{y}{216}\right) \end{array} \quad .$$

transformant l'équation (4.2) en l'équation simplifiée de Weierstrass

$$E\,:\, y^2 = x^3 + Ax + B$$

où $A = -27c_4$, $B = -54c_6$, avec

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 26b_2b_6$$
$$b_2 = a_1 + 4a_2, \quad b_4 = a_4 + 4a_1a_3, \quad b_6 = a_3^2 + 4a_6$$

de discriminant

$$\Delta = -16\left(4A^3 + 27B^2\right) \neq 0$$

La condition $\Delta = \Delta_E \neq 0$ assure que E n'a pas de point singulier. L'ensemble $E\left(K\right)$ des points K-rationnels de E est donné par

$$E\left(K\right) = \left\{(x, y) \in K^2\,;\, f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6\right\} \cup \left\{0_E\right\}$$

où $a_1, a_2, a_3, a_4, a_6 \in K$.

Un point $P = (a, b) \in E(K)$ est dite singulier si est seulement si

$$\frac{\partial f}{\partial x}\left(a, b\right) = \frac{\partial f}{\partial y}\left(a, b\right) = 0$$

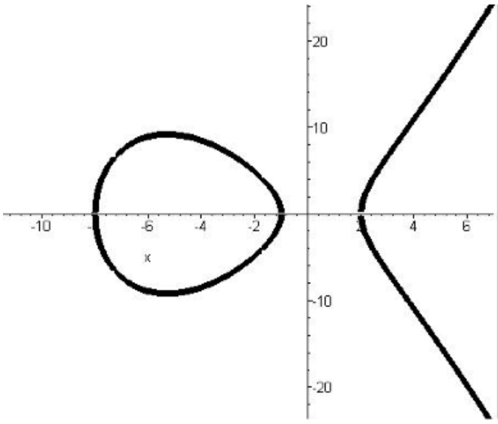
La courbe E et dite lisse si $\dfrac{\partial f}{\partial x}\left(a, b\right)$ et $\dfrac{\partial f}{\partial y}\left(a, b\right)$ ne s'annulent pas simultanément, pour tout point (x, y) sur la courbe.

— Si $\Delta > 0$, alors le polynôme cubique $x^3 + Ax + B$ a exactement trois racines réelles distinctes.

Exemple 4.1. Considérons la courbe d'équation

$$y^2 = (x+8)(x+1)(x-2)$$

dont le graphe est



avec $\Delta = 705600$

$$\begin{cases} \dfrac{\partial\left(y^2-(x+8)(x+1)(x-2)\right)}{\partial x}(a,b) & = 0 \\ \dfrac{\partial\left(y^2-(x+8)(x+1)(x-2)\right)}{\partial y}(a,b) & = 0 \end{cases} \Rightarrow \begin{cases} a = & \frac{-7\pm\sqrt{79}}{3} \\ b = & 0 \end{cases}$$

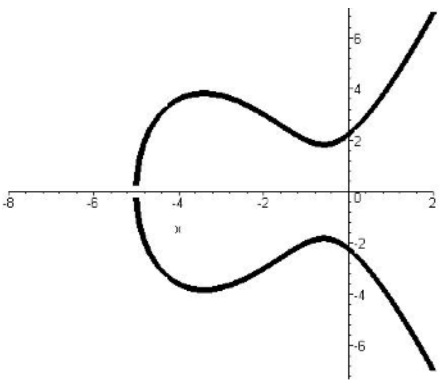
où les points $\left(\dfrac{-7\pm\sqrt{79}}{3}, 0\right)$ ne sont pas sur la courbe, alors la courbe est non-singulière, elle est dite lisse.

— Si $\Delta < 0$, alors le polynôme cubique $x^3 + Ax + B$ a exactement une racine réelle.

Exemple 4.2. Considéron l'équation

$$y^2 = \left(x^2+x+1\right)(x+5)$$

dont la courbe est



avec $\Delta = -21168$

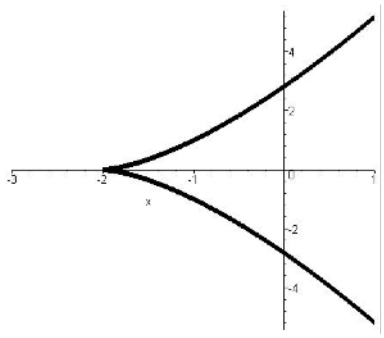
Alors on a

$$\begin{cases} \dfrac{\partial\left(y^2-(x^2+x+1)(x+5)\right)}{\partial x}(a,b) & = 0 \\ \dfrac{\partial\left(y^2-(x^2+x+1)(x+5)\right)}{\partial y}(a,b) & = 0 \end{cases} \Rightarrow \begin{cases} a = & -2\pm\sqrt{2} \\ b = & 0 \end{cases}$$

où les points $\left(-2 \pm \sqrt{2},\, 0\right)$ ne sont pas sur la courbe, alors la courbe est non-singulière, elle est dite lisse.

— Si $\Delta = 0$, la courbe E n'est pas elliptique

Exemple 4.3. Considérons les courbes suivantes

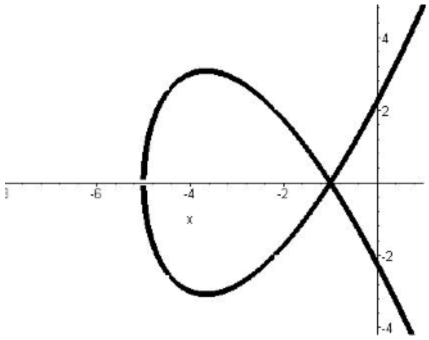


$$y^2 = (x+2)^3,\ \Delta = 0$$

$$\begin{cases} \dfrac{\partial\left(y^2-(x+2)^3\right)}{\partial x}(a,b) = 0 \\ \dfrac{\partial\left(y^2-(x+2)^3\right)}{\partial y}(a,b) = 0 \end{cases}$$

de point singulier $(-2, 0)$ sur la courbe

La courbe est dite non lisse



$$y^2 = (x+1)^2\,(x+5),\ \Delta = 0$$

$$\begin{cases} \frac{\partial\left(y^2-(x+1)^2(x+5)\right)}{\partial x}(a,b) = 0 \\ \frac{\partial\left(y^2-(x+2)^2(x+5)\right)}{\partial y}(a,b) = 0 \end{cases}$$

de point singulier $(-1, 0)$ sur la courbe

La courbe est dite non lisse

4.1.3 Invariant d'une courbe elliptique

Une courbe algébrique E est une courbe elliptique si est seulement si son discriminant $\Delta_E \neq 0$. Dans ce cas, on pose

$$j\,(E) = -1728\frac{(4A)^3}{\Delta_E}$$

appelé j-invariant de E.

Proposition 4.1. *[27]*

Deux modèles de Weierstrass simplifiés sont dit $\bar{K}$ -isomorphes si est seulement si ils ont le même j-invariant.

Etant donné que $j_0 \in K$, il existe un modèle de Weierstrass sur K de j-invariant égal à j_0. Il y a une autre forme d'équation de Weierstrass, dite de Legendre , donnée par

Définition 4.4. [27]

Une équation de Weierstrass est dans la forme de Legendre si elle peut s'écrire

$$y^2 = x(x-1)(x-\lambda).$$

Proposition 4.2. *[6]*

Supposons que car$(K) \neq 2$, alors

- *chaque courbe elliptique est isomorphe (sur $\bar{K}$) à une courbe elliptique dans la forme de Legendre est*

$$E_\lambda \,:\, y^2 = x(x-1)(x-\lambda)$$

pour certain $\lambda \in \bar{K}$ avec $\lambda \neq 0, 1$.

- *Le j-invariant de E_λ est*

$$j\left(E_\lambda\right) = 2^8 \frac{\lambda^2 - \lambda + 1}{\lambda\left(\lambda - 1\right)^2}.$$

4.1.4 Représentation projective

Les points K-rationnels du plan projectif $\mathbb{P}^2(K)$ sont les points projectifs donnés par les classes d'équivalences du triplet $(X, Y, Z) \in K^3 - ((0,0,0))$ sous l'action de multiplication sur K^* :

$$(X_1, Y_1, Z_1) \approx (X_2, Y_2, Z_2) \text{ si } X_1 = \lambda X_2,\, Y_1 = \lambda Y_2,\, Z_1 = \lambda Z_2$$

pour $\lambda \in K^*$. Ainsi, le point $P\left(x, y\right)$ en coordonnées projectives donne

$$(X, Y, Z) = \left(XZ^{-1}, YZ^{-1}, 1\right)$$

et en représentation en représentation affine donne

$$(x, y) = \left(\frac{X}{Z}, \frac{Y}{Z}\right).$$

Lorsque $Z = 0$, on a $X = 0$ et on écrit

$$(X, Y, Z) = (0, Y, 0) \neq (0, 0, 0)$$

et comme $(X, Y, Z) \in K^3 - (0, 0, 0)$,alors

$$(0, Y, 0) = Y\left(0, 1, 0\right).$$

On obtient le point à l'infini en coordonnées affines correspondant au point $(0, 1, 0)$ en coordonnées projectives.

4.1.5 Loi de groupe

Soit E une courbe elliptique définie sur un corps K, il existe une loi d'addition appelée sécante-tangente qui pour deux points de E associe un troisième point de E. L'ensemble des points $E(K) \bigcup O_E$ munie de cette loi forme un groupe commutatif. La règle d'addition est notée $+$.

Théorème 4.1. *[3] (Bézout simplifié)*
Soit C_1 et C_2 deux courbes définies sur un corps algébriquement clos K d'équation respectives $F(x,y) = 0$ et $G(x,y) = 0$. Alors le nombre de points, en comptant leurs multiplicités, qui se trouvent dans l'ensemble $C_1 \bigcap C_2$ est

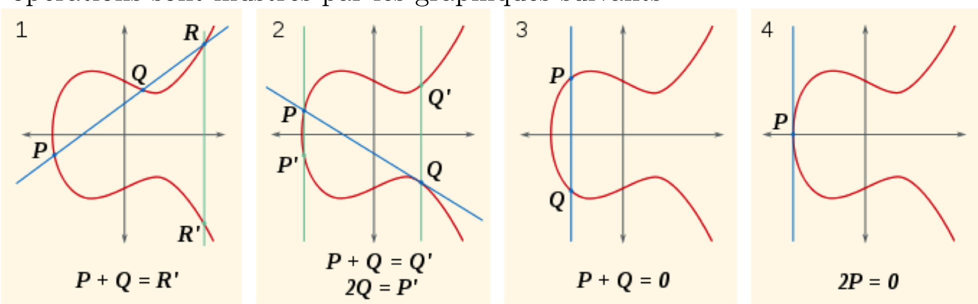
$$|(C_1 \cap C_2)| = \deg(C_1) \, . \deg(C_2)$$

En particulier, si $C_1 = E$ est une courbe elliptique et $C_2 = D$ est une droite alors $|C_1 \bigcap C_2| = 3$.

A partir du théorème de Bézout, on déduit que le nombre de points d'intersections entre une droite et une courbe elliptique est au plus 3. Grace à ce résultat on peut définir une opération de groupe, définie de façon géométrique.

- **L'opposé d'un point** $-P = R$: on trace une droite parallèle à l'axe des ordonnées passant par le point P, alors R est le second point d'intersection, autre que P, de la droite et de la courbe.
- **La somme de deux points** $P + Q = R$: on trace une droite passant par les deux points P et Q, alors R est l'opposé du point d'intersection entre la droite et la courbe.
- **Le doublement d'un point** $2P = R$: on trace la droite tangente à la courbe passant par P, alors R est l'opposé du point d'intersection de la courbe et de la droite.

Ces opérations sont illustrés par les graphiques suivants



On peut transposer cette description géométrique de façon algébrique, et selon la nature du corps de base la formule d'addition diffère.

Soit $K = \mathbb{Q}$, en considérant la forme simplifiée de l'équation de Weierstrass, la loi d'addition sur $E/\mathbb{Q}$ est donnée par :

- Identité : $P + O_E = O_E + P = P$ pour tout $P \in E/\mathbb{Q}$
- Opposé : si $P = (x,y) \in E/\mathbb{Q}$, alors $P + (-P) = O_E$ avec $-P = (x, -y)$ le point opposé de P.

— Addition de points : soient $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ deux points de $E/\mathbb{Q}$ et Soit $R = P_1 + P_2 = (x_3, y_3)$, avec $P_2 \neq -P_1$ (sinon $P_1 + P_2 = 0_E$).

Supposons tout d'abord$P_2 \neq P_1$. La droite passant par P_1 et P_2 a pour équation $y = \alpha x + \beta$ avec $\alpha = \dfrac{y_2 - y_1}{x_2 - x_1}$ et $\beta = y_1 - \alpha x_1$ (Remarquons que α est bien défini car si $x_2 = x_1$ alors $P_1 = \pm P_2$ ce qui est exclu par hypothèse). L'intersection de la droite (P_1P_2) avec la courbe E est donnée par :

$$(\alpha x + \beta)^2 = x^3 + Ax + B,$$

ce qui donne l'équation suivante :

$$x^3 - \alpha^2 x^2 + (A - 2\alpha\beta)\, x + \left(B - \beta^2\right) = 0$$

dont on connait deux solutions, à savoir x_1 et x_2. Or la somme de trois racines est l'opposé du coefficient de degré 2 et on pose donc :

$$\begin{cases} x_3 = \alpha^2 - x_1 - x_2 & . \\ y_3 = \alpha\,(x_1 - x_3) - y_1 & \end{cases}$$

— Doublement de point : Supposons maintenant que $P_1 = P_2 = (x_1, y_1)$. La droite tangente à la courbe E au point P_1 a pour équation $y = \alpha x + \beta$ avec $\alpha = \dfrac{3x_1^2 + A}{2y_1}$ et $\beta = y_1 - \alpha x_1$.

(Remarquons que α est bien défini car si $y_1 = 0$ alors $P_1 = -P_1$, ce qui est exclu par hypothèse). l'intersection de la droite avec la courbe E est donnée par :

$$(\alpha x + \beta)^{\,2} - x^3 - Ax - B = 0$$

ce qui donne l'équation suivante

$$x^3 - \alpha^2 x^2 + (A - 2\alpha\beta)x + (B - \beta^2) = 0$$

dont on connait deux solutions, à savoir x_1 et x_2. Or la somme de trois racines est l'opposé du coefficient de degré 2 et on pose donc :

$$\begin{cases} x_3 = \alpha^2 - 2x_1 & . \\ y_3 = \alpha\,(x_1 - x_3) - y_1 & \end{cases}$$

4.1.6 Courbe elliptique sur le corps $\mathbb{Q}$ des nombres rationnels

Si deux points ont des coordonnées rationnelles, la droite qui les joint a une équation à coefficient rationnels et le troisième point d'intersection avec la courbe est encore à coordonnées rationnelles. Le théorème de Mordell-Weil nous assure que le groupe des points rationnels est de type fini.

Théorème 4.2. *(Mordell.Weil .[6]*

Si E est une courbe elliptique définie sur le corps des nombres rationnels $\mathbb{Q}$, le groupe des points rationnels $E(\mathbb{Q})$ est de type fini. Alors il existe un nombre fini de points $P_1, P_2, \cdots, P_n \in E(\mathbb{Q})$ tels que tout point P de $E(\mathbb{Q})$ s'écrit sous la forme

$$P = m_1 P_1 + \cdots + m_n P_n, \quad m_i \in \mathbb{Z},\, 1 \leq i \leq n.$$

Définition 4.5. [17] (Rang d'une courbe elliptique)

Le rang d'une courbe elliptique est le nombre de points d'ordre infini indépendant.

Définition 4.6. [17] (Point de torsion d'une courbe elliptique).

L'ensemble des points de torsion d'une courbe elliptique E/K est

$$E(K)_{tors} = \{P \in E(K),\, \exists m \in \mathbb{N}^* \text{ tel que } mP = 0_E\}$$

qui est un ensemble de points de E d'ordre fini.

Selon les définitions précédentes, on a $E(\mathbb{Q})$ est le produit direct d'un nombre fini de copies de $\mathbb{Z}$ et de groupes cycliques finis de type $\mathbb{Z}/m\mathbb{Z}$. Alors

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{tors}$$

où $r \in \mathbb{N}$ et est appelé rang de E.

Exemple 4.4. . Soit la courbe elliptique $E/\mathbb{Q}$ défini par

$$E\,:\, y^2 = x^3 - 82x.$$

L'ensemble des points $\mathbb{Q}$- rationnels de E est

$$E(\mathbb{Q}) = < (0,0), (-8,12), (-1,-9), (-9,-3) >,$$

où $(0,0)$ est un point d'ordre 2 et les autres sont d'ordre infini. Alors

$$E(\mathbb{Q}) \simeq \mathbb{Z}^3 \times \mathbb{Z}/2\mathbb{Z}$$

ce qui veut dire que E est de rang 3.

4.1.7 Points entiers

Maintenant, combien de points rationnels sur une équation de Weierstrass donné (affine) ont des cordonnées entiers ?

Théorème 4.3. *[28] (Carl Siegel)*
L'ensemble des points $P(x,y)$ de $E(\mathbb{Q})$, tels que x soit un entier, est fini.

Si l'équation de Weierstrass de la courbe a des coefficients entiers plus petits qu'une constante H, les coordonnées (x,y) d'un point de la courbe telles que x et y soient entiers, vérifient

$$\mathrm{Max}(|x|,|y|) < exp\left(\left(10^6 H\right)^{10^6}\right)$$

Théorème 4.4. *(Baker [27])*
Soient $A,B,C,D \in \mathbb{Z}$ qui satisfont

$$Max\{|A|,|B|,|C|,|D|\} \leq H$$

et admettant que

$$E\,:\,Y^2 = AX^3 + BX^2 + CX + D$$

est une courbe elliptique. Si $P = (x,y) \in E(\mathbb{Q})$ avec $x,y \in Z$, alors

$$Max(|x|,|y|) < exp\left(\left(10^6 H\right)^{10^6}\right)$$

Démonstration. (voir [27]) □

L'un des résultats centraux de l'arithmétique des courbes elliptiques est le théorème de Lutz – Nagell suivant

Théorème 4.5. *[31]*
Soit $E/\mathbb{Q}$ une courbe elliptique à coefficients entiers. Si $P = (x,y)$ est un point de torsion de E, alors $x,y \in \mathbb{Z}$ et $y = 0$ ou $y^2 \mid \Delta$.

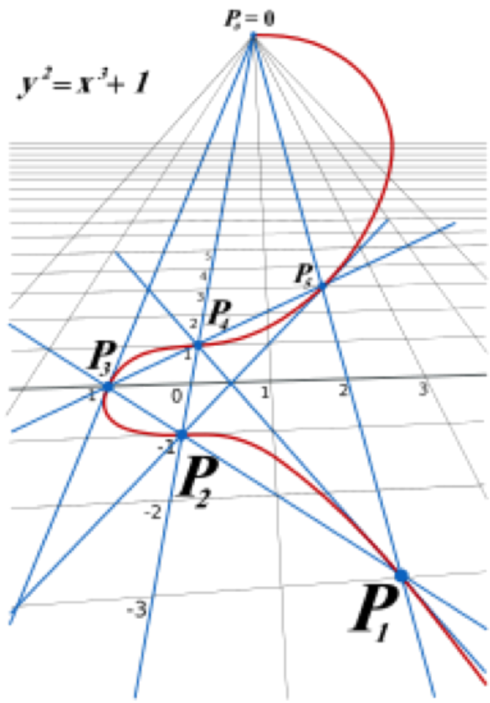
En fait, si E est la courbe elliptique défini suivant un modèle affine sur $\mathbb{Q}$ par

$$E\,:\,y^2=f\left(x\right)=x^3+Ax+B,\qquad A,B\in\mathbb{Z}$$

alors tout point de torsion non trivial $P=(a,b)\in E\left(\mathbb{Q}\right)$, alors a et b sont des entiers, et si $b\neq 0$, en d'autre termes P n'est pas d'ordre 2, on aura b^2 divise $-\left(4A^3+27B^2\right)$.

Exemple 4.5. Soit E l'équation elliptique définit sur $K=\mathbb{R}$ par

$$Y^2=x^3+1$$



On a

$$P_1=(2,-3)=5P_5$$

$$P_2=(0,-1)=4P_5$$

$$P_3=(-1,0)=3P_5$$

$$P_4=(0,1)=2P_5\,\text{(point double)}$$

$$P_5=(2,3)=1P_5$$

$$P_6=0_E=6P_5.$$

Alors le groupe de torsion

$$\begin{aligned} E\left(K\right)_{tors} &= \{0_E,\, P_1,\, P_2,\, P_3,\, P_4,\, P_5\} \\ &= \{kP_5,\, 1 \leq k \leq 6\} \\ &= \langle P_5 \rangle \end{aligned}$$

est un groupe cyclique d'ordre 6, ce qui entraine

$$E\left(K\right)_{tors} \simeq \mathbb{Z}/6\mathbb{Z}\,(\text{ le rang de } E \text{ est égal à } 0)\,.$$

Exemple 4.6. L'équation de Weierstrass

$$E\,:\, y^2 = x^3 + 43x + 166$$

est de discriminant

$$4A^3 + 27B^2 = 425984 = 2^{15}.13.$$

Tout point $P \in E(\mathbb{Q})$ tel que $x(P)$ et $x(2P)$ sont les deux entiers ayant la propriété que

$$y^2 \text{ divise } 2^{15}.13$$

Par conséquent, tout point de torsion dans $E(\mathbb{Q})$ a son ordonnée y dans l'ensemble

$$\left\{0,\, \pm 1,\, \pm 2,\, \pm 2^2, \ldots,\, \pm 2^7\right\}$$

et un simple calcul permet de révéler les points

$$\{(3, \pm 8)\,,\, (-5, \pm 16)\,,\, (11, \pm 32)\}$$

4.2 L'EQUATION DIOPHANTIENNE $h(a)x^2 + f(a) = g(a)a^n$

4.2.1 Introduction

Li et Yuan [20] ont considéré l'équation diophantienne

$$\left(a-1\right)x^2 + \left(91a + 9\right) = 4a^n \tag{4.3}$$

Où $a > 1$, x et n sont des entiers positifs, et ont prouvé que si $a = 5$, alors l'équation (4.3) a une solution unique $(x, n) = (3, 3)$.

Mua Hua-Le [11] a remarqué que si $a = 7$, alors l'équation (4.3) a comme solution $(x, n) = (11, 3)$. Par la suite, ils a considéré l'équation

$$(a-1)\, x^2 + f\,(a) = 4a^n \tag{4.4}$$

où $f(a)$ est une expression polynomiale en a non négative telle que

$$f\,(1) = 2^r p + 4, \quad r \in \mathbb{N}$$

où p est un nombre premier de Mersenne.

Clairement, en posant $f(a) = 91a + 9$, alors pour $p = 3$ et $r = 5$ on a bien $f\,(1) = 100 = 2^5 \times 3 + 4$, ce qui en fait de l'équation (4.4) une généralisation de l'équation (4.3) .

Il a été prouvé dans [11] que l'équation (4.4), sous la condition $f(a)$, admet un nombre fini de solutions, et celles-ci sont toutes trouvées. Notons que dans cet article l'une des solutions trouvée est fausse. En effet, la dernière solution devrait être (3,2), et non pas (3,4), comme nous le verrons dans la troisième partie de ce chapitre.

Dans ce chapitre, nous allons considérer l'équation diophantienne plus générale

$$h(a)x^2 + f(a) = g(a)a^n \tag{4.5}$$

où h, f et g sont des polynômes en $a > 1$ à coefficients entiers tels que

$$h(1) = 0, f(1) \neq g(1).$$

En prenant

$$h(a) = a - 1, \quad g(a) = 4$$

on obtient l'équation (4.4).

Il est clair que l'équation (4.5) est une généralisation de l'équation (4.4). En fait, nous n'avons pas besoin comme dans [?] que les coefficients de f soient non-négatifs.

Pour montrer que l'équation (4.5) n'a qu'un nombre fini de solutions et donner une borne efficace pour ces solutions, nous utiliserons la théorie des courbes elliptiques et le fameux théorème de Baker sur le nombre de points entiers sur une courbe elliptique à coefficients entiers. Nous expliquerons comment on peut expliciter toutes ces solutions et à titre d'exemple, nous considérerons l'équation (4.3).

4.2.2 Sur l'équation $h(a)x^2 + f(a) = g(a)a^n$

Puisque$h(1) = 0$, en prenant l'équation (4.5) modulo $(a-1)$, on obtient

$$f(1) \equiv g(1) \,(\mathrm{mod}(a-1))$$

ce qui donne

$$(a-1) \mid (f(1) - g(1)) \,. \tag{4.6}$$

Comme $f(1) \neq g(1)$, alors la relation (4.6) fournit toutes les valeurs possibles de l'entier a, qui sont au nombre fini.

Nous obtenons le résultat principal suivant

Théorème 4.6. *l'équation (4.5) a un nombre fini de solutions. De plus, si $h(a)f(a)g(a) \neq 0$, alors nous avons*

$$a < |f(1) - g(1)| + 1,$$

$$|x| < \max_{m=0,1,2} \left\{ \frac{exp\left(10^6 h(a)^3 g(a)^2 a^{2m} f(a)\right)^{10^6}}{h(a)^2 \,|g(a)|\, a^m} \right\}$$

et

$$|n| < \max_{m=0,1,2} \left\{ 3 \frac{\left(10^6 h(a)^3 g(a)^2 a^{2m} f(a)\right)^{10^6} - \ln\left(|h(a)g(a)|\, a^m\right)}{\ln(a)} + m \right\}$$

Démonstration. La relation (4.6) implique que

$$-\,|f(1) - g(1)| \leq a - 1 \leq |f(1) - g(1)| \,,$$

ce qui donne

$$-\,|f(1) - g(1)1| + 1 \leq a \leq |f(1) - g(1)| + 1,$$

et entraine que

$$|a| \leq |f(1) - g(1)| + 1.$$

Pour obtenir les majorations données dans le théorème, nous considérerons les valeurs de n suivant leurs classes modulo 3. Dans chacun des cas à considérer, nous écrirons a^n sous la forme $\left(a^{(n-k)/3}\right)^3$ avec $k \equiv n$ mod 3.

Cas 1. $n \equiv 0\,(\mathrm{mod}\ 3)$. En multipliant l'équation (4.5) par $h(a)^3 g(a)^2$, on obtient

$$\left(h(a)^2 g(a) x\right)^2 + h(a)^3 g(a)^2 f(a) = \left(h(a) g(a) a^{n/3}\right)^3 .$$

Soit

$$Y = h(a)^2 g(a) x \text{ et } X = h(a) g(a) a^{n/3}$$

ils vérifient une relation, l'équation d'une courbe elliptique, donnée par

$$E_A : Y^2 = X^3 - A$$

où

$$A = h(a)^3 g(a)^2 f(a).$$

Comme $h(a)f(a)g(a) \neq 0$, alors $A \neq 0$. Notons ici que, toute solution entière (x, n) de l'équation (4.5) donnera lieu à un point entier sur cette courbe elliptique E_A. Par le théorème de Seigle [28], on sait qu'il y a un nombre fini de points entiers (notez que A est un entier). Le théorème 4.4 implique que (X,Y) satisfait

$$\text{Max}\{|X|, |Y|\} < \exp\left(\left(10^6 A\right)^{10^6}\right),$$

alors

$$|x| < \frac{\exp\left(\left(10^6 A\right)^{10^6}\right)}{h(a)^2 |g(a)|}$$

et

$$n < 3\frac{\left(10^6 A\right)^{10^6} - \ln(|h(a) g(a)|)}{\ln(a)}$$

Cas 2. $n \equiv 1 \pmod 3$. En multipliant l'équation (4.5) par $h(a)^3 g(a)^2 a^2$, on aura

$$\left(h(a)^2 g(a).a.x\right)^2 + h(a)^3 g(a)^2.a^2.f(a) = \left(h(a)g(a).a.a^{(n-1)/3}\right)^3.$$

Soit

$$Y = h(a)^2 g(a) a x,$$

et

$$X = h(a) g(a).a.a^{n-1/3},$$

on obtient de nouveau la courbe elliptique

$$E_A : Y^2 = X^3 - A$$

avec $A = h(a)^3 g(a)^2 a^2 f(a)$.

Comme $h(a)f(a)g(a) \neq 0$, alors $A \neq 0$, par le même raisonnement que dans le cas 1, et en utilisant le théorème 4.4 et les formules de X et Y, on aura

$$|x| < \frac{\exp\left(\left(10^6 A\right)^{10^6}\right)}{h\left(a\right)^2 \left|g\left(a\right)\right| a}$$

et

$$n < 3\frac{\left(10^6 A\right)^{10^6} - \ln\left(\left|h\left(a\right) g\left(a\right)\right| a\right)}{\ln\left(a\right)} + 1.$$

Cas 3. $n \equiv 2 \pmod 3$. En multipliant l'équation (4.5) par $h(a)^3 g(a)^2 a^4$, nous obtenons

$$\left(h(a)^2 g(a) a^2 x\right)^2 + h(a)^3 g(a)^2 a^4 f(a) = \left(h(a) g(a) a^2 a^{(n-2)/3}\right)^3.$$

Soit

$$Y = h(a)^2 g(a) a^2 x,$$

et

$$X = h\left(a\right) g(a).a^2.a^{n-2/3},$$

on obtient de nouveau la courbe elliptique

$$E_A : Y^2 = X^3 - A$$

avec $A = h(a)^3 g(a)^2 a^4 f(a)$.

Comme $h(a)f(a)g(a) \neq 0$, alors $A \neq 0$, par le même raisonnement que dans le cas 1, et en utilisant le théorème 4.4 et les formules de X et Y, on aura

$$|x| < \frac{\exp\left(\left(10^6 A\right)^{10^6}\right)}{h\left(a\right)^2 \left|g\left(a\right)\right| a^2}$$

et

$$n < 3\frac{\left(10^6 A\right)^{10^6} - \ln\left(\left|h\left(a\right) g\left(a\right)\right| a^2\right)}{\ln\left(a\right)} + 2.$$

Comme ils n'y a qu'un nombre fini de valeur de a, nous pouvons prendre le maximum des valeurs finies des bornes pour obtenir les bornes absolues données dans le théorème.

$\square$

4.2.3 Sur l'équation $(a-1)x^2 + (91a+9) = 4a^n$.

Nous allons maintenant considérer l'équation (4.3) et expliciter toutes ses solutions.
Mu Hua-Le [11] a montré que toutes ces solutions sont

$$(x, n) = (3, 3), (11, 3), (3, 4)$$

pour $a = 5, 7, 25$ respectivement. Comme mentionné précédemment, la dernière solution $(3, 4)$ est en réalité $(3, 2)$.
Nous utilisons maintenant les résultats ci-dessus pour trouver toutes les solutions. Pour cela, commençons d'abord par noter que $f(1) = 100 \neq g(1) = 4$ et on a aussi $h(1) = 0$ comme demandé. De la relation (4.6) on en déduit que

$$a \in \{2, 3, 4, 5, 7, 9, 13, 17, 25, 33, 49, 97\}$$

Pour chaque valeur de a et pour chaque valeur de $n$modulo 3 nous avons mis en évidence une courbe elliptique correspondante E_A et pour chacune d'elles nous avons déterminé les points entiers en utilisant l'algorithme de Magma du groupe Mordell-Weil [4]. Pour chaque point entier (X, Y) trouvé, nous avons utilisé les formules de reconversion pour X et Y, données ci-dessus, afin de de déterminer les solutions et dont les résultats sont résumés dans le tableau ci-dessous.

Remarque 4.1. Comme les courbes elliptiques sous cette forme sont symétriques par rapport à l'axe des abscisses, chaque point entier trouvé correspond à 2 solutions de la courbe elliptique : l'une avec un ordonnée Y positive, et l'autre avec un ordonnée Y négative. Cependant, en observant la formule pour Y, on voit que le changement du signe de Y entraine le changement du signe de x, qui est carré dans l'équation. Ces solutions supplémentaires sont évidentes, nous ne listons donc que celles à ordonnées y positives.

Valeur de a	$n \mod 3$	Valeur de A	Point entiers sur E_A
2	0	3056	Aucun
2	1	12224	$[24, 40]$, $[1020, 32576]$ $[3240, 184424]$
2	2	48896	$[368, 7056]$
3	0	36096	Aucun
3	1	324864	$[760, 20944]$
3	2	2923776	Aucun

Valeur de a	$n \mod 3$	Valeur de A	Point entiers sur E_A
4	0	161136	Aucun
4	1	2578176	$[160, 232]$
4	2	41250816	$[448, 6976]$, $[1120, 36928]$
5	0	475136	$[80, 192]$, $[96, 640]$, $608, 14976$ $[2340, 113191]$, $[2528, 127104]$
5	1	11878400	Aucun
5	2	296960000	Aucun
7	0	2232576	$[168, 1584]$
7	1	296960000	Aucun
7	2	2232576	$4776, 321840$
9	0	6782976	Aucun
9	1	549421056	$[8928, 843264]$
9	2	44503105536	Aucun
13	0	32956416	Aucun
13	1	5569634304	Aucun
13	2	941268197376	Aucun
17	0	101974016	Aucun
17	1	29470490624	Aucun
17	2	8516971790336	Aucun
25	0	505184256	$[1680, 65088]$
25	1	315740160000	$[1680, 65088]$

Valeur de a	$n \mod 3$	Valeur de A	Point entiers sur E_A
25	2	197337600000000	$[4119625, 8361533125]$ $[60000, 4320000]$ $[1442500, 1732445000]$
33	0	1579155456	$[1168, 3776]$, $[1408, 34816]$ $[223360, 105562112]$
33	1	1719700291584	Aucun
33	2	1872753617534976	Aucun
49	0	7906000896	Aucun
49	1	18982308151296	$[113680, 38080448]$
49	2	45576521871261696	Aucun
97	0	125080436736	Aucun
97	1	1176881829249024	Aucun
97	2	7373462942305484800	Aucun

On en déduit que les solutions sont :

— $(x, n) = (3, 3)$ correspondant à $(X, Y) = (80, 192)$ où $a = 5$,

— $(x, n) = (11, 3)$ correspondant à $(X, Y) = (168, 1584)$ où $a = 7$,

— et $(x, n) = (3, 2)$ correspondant à $(X, Y) = (60000, 4320000)$ où $a = 25$.

Remarque 4.2. La condition $h(a)g(a) \neq 0$ dans le Théorème 4.6 n'est pas restrictive. En fait, si a est un entier positif tel que $h(a) = 0$, alors l'équation (4.5) donne

$$f(a) = g(a)a^n,$$

ce qui peut être facilement résolu pour chaque racine a du polynôme h .

De même, si $g(a) = 0$, alors l'équation (4.5) donne l'équation quadratique en x

$$h(a)x^2 + f(a) = 0$$

qui peut être facilement résolue pour chaque racine a du polynôme g.

Remarque 4.3. À travers ce chapitre, nous avons supposé que a est positif. Nous pouvons assouplir cette condition et autoriser des valeurs négatives. Pur cela, nous avons juste besoin de remplacer a par $|a|$, et la même méthode que nous avons utilisé ci-dessus s'applique si nous supposons $h(-1) = 0$ et $f(-1) \neq g(-1)$.

Bibliographie

[1] S. A.Alkabouss, B. Benseba, N. Berbara and O. Kihel, A note On the diophantine equation$x^2 - kxy + ky^2 + ly = 0$, 2019 (soumis).

[2] N. Berbara, O. Kihel, S. Mavecha, and J. Midgley. On the diophantine equation $h(a)x^2 + f(a) = g(a)a^n$. Accepté pour publication dans Functiones and Approximato, commentary Mathématic (2019).

[3] A. Berenger et E. Ayebie.courbe elliptiques : formules d'addition et de doublement unifiées (2012)

[4] W. Bosma, J. Cannon, and C. Playoust, The Magma al- gebra system. I. The user language, J. Symbolic Comput., 24 (1997), 235-265. N

[5] W. Burton, M.David : Elementary number theory,1980. Allyn and Bacon,Inc.

[6] S. M. Chiarello et M. Chaminadour : Le théorème de Mordell pour les courbes elliptiques. juin 2014.(1-16)

[7] R.Férréol et F.Casiro, Olympiades et concours général de mathématiques. (énoncés et corrigés) de 1983 à 1987.

[8] D. Goffinet. Exercices corrigés de mathématiques, math sup, capes, agregation de Mathématiques (deux volumes).

[9] D. Grant. On an analogue of the Lutz–Nagell Theorem for hyperelliptic curves.2012.

[10] G.Gras,M-N.Gras, Algèbre fondamentale Arithmétique, 2004. Ellipses.

[11] Mua Hua-Le, A note on the diophantine equation $(a-1)x^2 + f(a) = 4a^n$, Acta Mathematica Sininca, Chinese Series 54 (2011), no. 1, 111- 114.

[12] Y. Hu and M. Le, On the Diophantine equation $x^2 - kxy + y^2 + lx = 0$, Chin. Ann. Math 34B (5) (2013), 715-718.

[13] O. Karaatli and Z. Siar ; On the Diophantine equations $x^2 - kxy + ky^2 + ly = 0,\ l \in 1; 2; 4, 8$; African Diaspora Journal of Mathematics 14 (2012), 24-29.

[14] R. Keskin Solutions of some quadratic Diophantine equations, Comput. Math. Appl.60 (2010), 2225-2230.

[15] R. Keskin, Z. Siar, and O. Karaatli, On the Diophantine equations $x^2 - kxy + y^2 + 2^n = 0$; Miskolc Mathematical Notes 13 (2012), n°2, 375-388.

[16] J.C. Lagarias, On the computational complexity of determining the solvability or unsolvability of the equation$X^2 - DY^2 = -1$, Trans. Amer. Math.Soc. 260 (1980), 480-508.

[17] O. Lecacheux. Rang de Familles de Courbes Elliptique.

[18] H. A. Lenstra, Algorithmic Number Theory MSRI Publications, Volume 44, 2008.

[19] H. W. Lenstra Jr, Solving the Pell equation, Notice of the AMS, Volume 49 (2) (2002), 182-192.

[20] Z. G. .Li and P. Z. Yuan , On the diophantine equation $(a-1)x^2 + (91a+9) = 4a^n$, Acta Mathematica Sinica, Chinese Series 53 (2010), no. 1, 37-44.

[21] A. Marlewski and P. Zarzycki, Infinitely many solutions of the Diophantine equation x^2-kxy + y^2 + x = 0, Comput. Math. Appl., 47 (2004), 115-121.

[22] S. Mavecha, On the Diophantine equation $x^2 - kxy + y^2 + lx = 0$,$l = 2^n$, Analele. Universiti deVest Timisoara Seria Matematic.-Informatic., LV,1 (2017), 115-118.

[23] R. A. Morlin, Simple continued fraction solutions for Diophantine equation, Expositions Mathematiae, 19 (2001), 55-73.

[24] R.Morlin, and A.Srinivasan A not on the Pell negative equation, Int J of Algebra,Vol 4 (2010), n19, 919-922.

[25] T. Nagell, Introduction to number theory, John Wiley & sons, Inc., New York, Stockholm 1951.

[26] C. Rithzenthaler : Introduction to elliptic curves. 2013-2014.(01-10).

[27] J. H. Silverman. The arithmetic of elliptic curves Springer-Verlag, 1985.

[28] J. .H.Silverman.Graduate Texts in Mathématics. The Arithmetic of Elliptic Curve.2010.

[29] S. Y. Yan, Number theory for computing, Berlin : Springer, 2000.

[30] P. Yuan and Y. Hu, On the Diophantine equation $x^2 - kxy + y^2 + lx = 0$,$l \in 1; 2; 4$ Comput. Math. Appl., 61 (2011), 573-577.

[31] J. Zinn-, Méthode algébriques en théorie des nombres,2010. Ellipse Edition.