



**UNIVERSITE MOHAMED BOUDIAF M'SILA**  
**Faculté de Mathématiques et Informatique**  
**Département de Mathématiques}**



## **MEMOIRE DE FIN D'ETUDE**

Présenté pour l'obtention du **Diplôme** de Master

**Domaine:** Mathématiques et Informatique

**Filière:** Mathématiques

**Option:** Algèbre et Mathématiques discrètes

**Par**

Chammah Ahmed

**Sujet**

**Résolution de quelques types  
d'équations diophantiennes**

**Devant le jury :**

<b>N. GHADBANE</b>	<b>MCA. Univ.M'SILA</b>	<b>Président</b>
<b>A. BOUDAUD</b>	<b>Pr. Univ.M'SILA</b>	<b>Encadreur</b>
<b>L. HEBOUB</b>	<b>MAA. Univ.M'SILA</b>	<b>Examineur</b>

**Promotion:2019/2020**

République Algérienne Démocratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

**UNIVERSITÉ MOHAMED BOUDIAF M'SILA**

**FACULTÉ DE MATHÉMATIQUES ET INFORMATIQUE**

**DÉPARTEMENT DE MATHÉMATIQUES**

Mémoire présenté en vue de l'obtention du Diplôme :

**MASTER en Mathématiques**

Option : Algèbre et Mathématiques Discrètes

Par

**Chammah Ahmed**

Titre :

# Résolution de quelques types d'équations diophantiennes

Devant les membres du Jury :

GHADBANE NACER	MCA .Univ.Msila	Président
BOUDAUD ABDELMADJID	Pr. Univ.Msila	Encadreur
HEBOUB LAKHDAR	MAA. Univ.Msila	Examineur

Septembre 2020

## DÉDICACE

Je dédie ce modeste travail à l'âme de mes parents.

A ma femme et mes enfants.

A mes frères et mes sœurs.

A toute la famille.

A tous mes amis et collègues.

## REMERCIEMENTS

- Je remercie Dieu qui m'a guidé à terminer ce travail et à l'écrire.
- Je tiens à remercier mon encadreur Mr. A. BOUDAUD de sa disponibilité, de ces conseils précieux tout au long de ce travail.
- Je tiens à exprimer mes sentiments à ma femme et mes enfants qui m'ont donné du courage pour terminer ce travail.
- Je tiens à exprimer mes respects à mes frères et sœurs qui m'ont encouragé.
- Je tiens à remercier tous les professeurs du département de mathématiques et ainsi que mes collègues, tous les étudiants et étudiantes de ma promotion.
- Je tiens à remercier les membres du jury, qui ont accepté d'évaluer mon travail de mémoire.

# Table des matières

<b>Remerciements</b>	ii
<b>Table des matières</b>	ii
<b>Introduction</b>	1
<b>1 Notions de bases</b>	3
1.1 Divisibilité . . . . .	3
1.2 Nombres premiers . . . . .	6
1.3 Congruences . . . . .	7
<b>2 Systèmes d'équations linéaires</b>	9
<b>3 Méthodes élémentaires pour la résolution d'équations diophantiennes</b>	18
3.1 Méthode de factorisation . . . . .	18
3.2 Méthode des inégalités . . . . .	20
3.3 Méthode paramétrique . . . . .	23
3.4 Méthode arithmétique modulaire . . . . .	24
3.5 Méthode d'induction . . . . .	25
3.6 Méthode de la descente infinie de Fermat . . . . .	27
<b>4 Quelques autre types d'équations diophantiennes</b>	29

<b>4.1</b> Equation $x^2 + y^2 = z^2$ . . . . .	29
<b>4.2</b> Equation $x^2 + y^2 = z^4$ . . . . .	29
<b>4.3</b> Equation $x^2 + (3y)^2 = z^2$ . . . . .	30
<b>4.4</b> Equation $(2x)^2 + y^4 = z^2$ . . . . .	30
<b>4.5</b> Equation $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$ . . . . .	31
<b>4.6</b> Equation $x^2 + y^2 = z^3$ . . . . .	31
<b>4.7</b> Equation $xz = y^2 + 1$ . . . . .	32
<b>4.8</b> Equation $x^2 + y^2 = u^2 + v^2$ . . . . .	33
<b>4.9</b> Equation $4^x + 18^y = 22^z$ . . . . .	33
<b>4.10</b> Equation $(x + y + z)xyz = u^2$ . . . . .	34
<b>4.11</b> Equation de Pell-Fermat . . . . .	35
<b>4.11.1</b> Méthode générale de résolution . . . . .	36
<b>4.11.2</b> Equation $ax^2 - by^2 = 1$ . . . . .	37
<b>4.11.3</b> Application 1 . . . . .	39
<b>4.11.4</b> Application 2 : . . . . .	39
<b>Bibliographie</b> . . . . .	41

# Introduction

Rappelons qu'une équation polynomiale à plus qu'une inconnue et dont les coefficients sont des entiers et les solutions sont des nombres entiers ou éventuellement des rationnels est appelée une équation diophantienne algébrique. C'est-à-dire elle prend la forme

$$f(x_1, x_2, \dots, x_n) = 0.$$

Où  $f$  elle est comme indiquée ci-dessus et  $n \geq 2$ . La branche des mathématiques concernée par la résolution et l'étude de telles équations est appelée l'arithmétique ou la théorie des nombres.

Diophantus est le premier à traiter ce genre d'équations où on trouve au jour d'hui son livre intitulé Arithmétiques comme un témoignage de cette époque.

Concernant la résolubilité d'une équation diophantienne, trois problèmes fondamentaux se posent : 1) L'équation est-elle résoluble ? 2) Si elle est résoluble. Le nombre de ses solutions est-il fini ou infini ? 3) La détermination de toutes ses solutions dans le cas où elle est résoluble.

Ce mémoire est formé par quatre chapitres.

**Le premier chapitre** : est consacré aux notions de base que l'on estime nécessaires pour le reste du mémoire.

**Le deuxième chapitre** : l'objet de ce chapitre est l'étude des systèmes linéaires diophantiens.

**Le troisième chapitre ;** on expose quelques méthodes élémentaires de résolution telles que méthode de factorisation, des inégalités, paramétriques.

**Le dernier chapitre :** est consacré aux quelques autres types d'équations diophantiennes.

# Chapitre 1

## Notions de bases

### 1.1 Divisibilité

**Définition 1.1.1** : On dit que l'entier non nul  $a$  divise l'entier  $b$  s'il existe un entier  $c$  tel que  $b = ac$ .

$a$  divise  $b$  sera notée  $a|b$ .

#### Propriétés

Si  $a$  est non nul et  $a$  divise  $b$  alors  $a|0$ .

Si  $a$  est entier alors  $1|a$ .

Si  $a|b$  et  $b|c$  alors  $a|c$ .

Si  $a|b$  et  $c$  entier non nul alors  $ac|bc$ ,  $a|b$  et  $a|bc$ .

Si  $a|b$  et  $a|c$ , alors pour tout entiers  $m, n$  on a  $a|mb + nc$ .

Si  $a|b$  et  $b|a$  alors  $a = \mp b$ .

Si  $a|b$  et  $a, b$  sont des entiers positifs alors  $a \leq b$ .

**Théorème 1.1.1** : Soient  $a, b$  des entiers et  $a$  positif, alors il existe un unique  $(q, r)$  tel que  $b = aq + r$  avec  $0 \leq r < a$ .

**Notation** (*Partie entière d'un réel*) : La partie entière du réel  $x$  notée  $[x]$ , est le seul entier  $n$  qui satisfait l'inégalité suivante  $n \leq x < n + 1$ .

**Exemple** :  $[7] = 7$ ,  $[4.33] = 4$ ,  $[-5.42] = -6$ .

**Corollaire 1.1.1** : Dans la division euclidienne on a  $q = \left[\frac{b}{a}\right]$  et  $r = b - a\left[\frac{b}{a}\right]$ .

**Définition 1.1.2** : Soit  $g$  un entier.  $g$  est un diviseur commun à  $a, b$  si  $g|a$  et  $g|b$ . Le plus grand diviseur commun de  $a$  et  $b$  est noté  $(a, b)$  ou  $PGCD(a, b)$ . Si  $a, b$  sont premiers entre eux on a  $(a, b) = 1$ .

**Théorème 1.1.2** : Soit  $g = (a, b)$  alors il existe deux entiers  $(x_0, y_0)$  tel que  $g = ax_0 + by_0$ .

**Lemme 1.1.1** : Si  $m$  est un entier, alors pour tout entiers  $a, b$  non nuls on a

$$(a, b) = (b, a) = (a, -b) = (a, b + am).$$

**Théorème 1.1.3** :  $(a, b)$  est le dernier reste non nul des divisions successives de l'algorithme d'Euclide.

**Exemple 1.1.1** : Soit à trouver  $(963, 657)$  et deux entiers  $(x_0, y_0)$  tels que  $(963, 657) = 963x_0 + 657y_0$ .

**Solution 1.1.1**

$$963 = 657 \times 1 + 306$$

$$657 = 306 \times 2 + 45$$

$$306 = 45 \times 6 + 36$$

$$45 = 36 \times 1 + 9$$

$$36 = 9 \times 4 + 0$$

Donc  $(963, 657) = 9$ .

$$9 = 45 - (306 - 45 \times 6) = -306 + 7 \times 45$$

$$9 = -306 + 7 \times (657 - 306 \times 2) = 7 \times 657 - 15 \times 306$$

$$9 = 7 \times 657 - 15 \times (963 - 657) = 963 \times (-15) + 657 \times 2$$

Alors  $(x_0, y_0) = (-15, 22)$  et  $(963, 657) = 963 \times (-15) + 657 \times (22)$ . On a une infinité d'entiers  $x, y$  tel que  $9 = 963x + 657y$ .

**Théorème 1.1.4** : Soient  $a, b$  deux entiers. On définit, pour  $k \geq 1$ , les deux suites  $\{s_k\}, \{t_k\}$  définies par  $s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$  et par les relations récurrentes :  $s_{k+1} = s_{k-1} - q_k s_k$  et  $t_{k+1} = t_{k-1} - q_k t_k$  où les  $q_k$  sont les quotients trouvées dans l'algorithme d'Euclide, où  $r_n$  est le dernier reste non nul, on a  $r_n = a s_{k+1} + b t_{k+1}$ .

**Exemple 1.1.2** : trouver  $x, y$  tels que  $963x + 657y = 9$ .

**Solution 1.1.2** On a  $q_1 = 1, q_2 = 2, q_3 = 6, q_4 = 1$ .

$$\begin{pmatrix} s_0 = 1 \\ s_1 = 0 \\ s_2 = 1 \\ s_3 = -1 \\ s_4 = 13 \\ s_5 = -15 \end{pmatrix}, \begin{pmatrix} t_0 = 0 \\ t_1 = 1 \\ t_2 = -1 \\ t_3 = -3 \\ t_4 = -19 \\ t_5 = 22 \end{pmatrix}.$$

Donc  $963 \times (-15) + 657 \times 22 = 9$

**Théorème 1.1.5** : Soit  $g = (a, b)$  alors les deux assertions suivantes sont équivalentes à la définition de  $g$

a)  $g = \min\{ax + by > 0 : x, y \in \mathbb{Z}\}$

b) Si  $d|a, d|b$  alors  $d|g$ .

**Théorème 1.1.6** : Si  $m$  est un entier positif alors  $(ma, mb) = m(a, b)$ .

**Corollaire 1.1.2** : Si  $d|a$  et  $d|b$ ,  $d > 0$  alors  $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{d}$ . En particulier si  $g = (a, b)$  alors  $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ .

**Corollaire 1.1.3** : Si  $c|ab$  et  $(b, c) = 1$  alors  $c|a$ .

## 1.2 Nombres premiers

**Définition 1.2.1** : L'entier  $p$  strictement supérieur à un est appelé un nombre premier si chaque fois que  $p = ab$  alors  $p = a$  ou  $p = b$ .

**Exemple** :  $p = 2, p = 7, p = 101, p = 541, \dots$

**Définition 1.2.2** : Chaque entier positif supérieur à un peut s'écrire comme produits de nombres premiers.

**Exemple** :  $a = 1800 = 2^4 \times 3^2 \times 5^2$

**Théorème 1.2.1** : Si  $n$  est composé alors il existe un nombre premier  $p$  tel que  $p \leq \sqrt{n}$  sachant que  $p|n$ .

**Théorème 1.2.2** : Il existe un infinité de nombre premiers.

**Théorème 1.2.3** (Théorème fondamentale de l'arithmétique) : Soit  $p$  un nombre premier. Si  $p|ab$  alors  $p|a$  ou  $p|b$ . Généralement si  $p|a_1 a_2 \dots a_n$  alors  $p|a_i$  pour un certain  $i, 1 \leq i \leq n$ .

**Théorème 1.2.4** (Factorisation unique, Théorème fondamentale de l'arithmétique) : Soit  $n > 1$  un entier. La factorisation de  $n$  en nombres premiers est unique à un ordre près.

**Exemple 1.2.1** : Trouver  $(480200, 121500)$ .

**Solution 1.2.1** On a  $480200 = 2^3 \times 5^2 \times 7^4$  et  $121500 = 2^2 \times 3^5 \times 5^3$ . Donc  $(480200, 121500) = 2^2 \times 5^2 = 100$ .

**Notation 1.2.1** (*Plus petit commun multiple*) : Le plus petit commun multiple de deux entiers  $a, b$  noté  $[a, b]$ .

**Corollaire 1.2.1** : Si  $a, b$  sont des entiers non nuls alors  $[a, b](a, b) = |ab|$ .

**Exemple 1.2.2** : Trouver  $[963, 657]$ .

**Solution 1.2.2** Comme  $[963, 657](963, 657) = 963 \times 657$ , alors  $[963, 657] = \frac{(963 \times 657)}{9} = 70299$ .

## 1.3 Congruences

**Définition 1.3.1** : Soient  $a, b$  des entiers et  $m$  un entier positif non nul. On dit  $a$  est congru à  $b$  modulo  $m$  si  $m|(a - b)$  et on écrit  $a \equiv b(\text{mod } m)$ .

**Exemple** :  $17 \equiv -3(\text{mod } 5)$ ,  $1 \equiv -6(\text{mod } 17)$ ,  $447 \equiv 21(\text{mod } 71)$ .

**Théorème 1.3.1** : Soit  $m$  un entier positif et soient  $a, b$  et  $c$  des entiers. Alors

i)  $a \equiv a(\text{mod } m)$ .

ii)  $a \equiv b(\text{mod } m)$  si et seulement si  $b \equiv a(\text{mod } m)$ .

iii) Si  $a \equiv b(\text{mod } m)$  et  $b \equiv c(\text{mod } m)$  alors  $a \equiv c(\text{mod } m)$ .

iv)  $m|a$  si et seulement si  $a \equiv 0(\text{mod } m)$ .

v) Si  $a \equiv b(\text{mod } m)$  et  $n$  un entier naturel alors  $a^n \equiv b^n(\text{mod } m)$ .

**Exemple 1.3.1** : Trouver le reste de la division euclidienne de  $A = 4444^{5555}$  par 13.

**Solution 1.3.1** : On a  $4444 \bmod 13 = 11$ , donc  $4444^{5555} \equiv 11^{5555} \bmod 13$ . Cherhons les restes de la division euclidienne de  $11^i$  par 13, où  $1 \leq i \leq 12$ .

$i$	1	2	3	4	5	6	7	8	9	10	11	12
$11^i$	11	4	5	3	7	12	2	9	8	10	6	1

D'autre part on a  $5555 = 462 \times 12 + 11$ . Donc le reste de la division euclidienne de  $11^{5555}$  par 13 est 6. Le reste de la division euclidienne de  $A = 4444^{5555}$  par 13 est 6.

**Théorème 1.3.2** : Si  $(m, n) = d$  alors  $ma \equiv mb \pmod{n}$  si et seulement si  $a \equiv b \pmod{\frac{n}{d}}$ .

**Corollaire 1.3.1** : Si  $(m, n) = 1$  alors  $ma \equiv mb \pmod{n}$  si et seulement si  $a \equiv b \pmod{n}$ .

# Chapitre 2

## Systemes d'equations lineaires

Soit le systeme suivant

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \dots \dots = \dots \dots (1) \\ \dots \dots \dots = \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{array} \right.$$

à  $m$  equations et  $n$  inconnues  $x_1, x_2, \dots, x_n$  et dont les coefficients  $a_{ij}$  ( $1 \leq i \leq m, 1 \leq j \leq n$ ) et les  $b_i$  ( $1 \leq i \leq m$ ) sont des entiers. Le systeme (1) peut être écrit sous la forme matricielle  $AX = B$  où  $A$  est la matrice  $m \times n$  suivante

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \text{ et } B = \begin{pmatrix} b_1 \\ b_2 \\ \dots \\ \dots \\ b_m \end{pmatrix}$$

est la matrice colonne  $m \times 1$ .

Le but dans cette section est d'étudier les solutions entieres de (1).

**Notation 2.0.1** *Pendant la résolution de (1) on va utiliser les opérations suivantes qui laissent les systèmes obtenus, durant le traitement, équivalents :*

(R1) *Ajouter un multiple entier  $m$  d'une équation à une autre ;*

(R2) *Échanger deux équations ;*

(R3) *Multiplier les deux côtés d'une équation par  $-1$  ;*

(C1) *Ajouter un multiple entier  $m$  d'une colonne à une autre ;*

(C2) *Échanger deux colonnes ;*

(C3) *Multipliez tous les éléments d'une colonne par  $-1$ .*

### Méthode pratique

On cherche un système équivalent à (1) de  $m$  équations en  $n$  variables équivalentes que l'on peut écrire sous la forme  $DY = B'$  où  $D$  est une matrice  $m \times n$  diagonale dans le sens où les nouveaux coefficients  $d_{ij} = 0$  lorsque  $i \neq j$ . Posons  $V = [v_{ij}]$  la matrice  $n \times n$  qui exprime nos variables originales en termes de nos nouvelles variables  $Y = [y_j]$  ( $1 \leq j \leq n$ ) alors  $VY = X$ . Initialement,  $V = I$ , la matrice d'identité. Nous donnons l'étape qui réduit  $A$  en une matrice  $A' = [a'_{ij}]$  avec la propriété que  $a'_{11} \geq 0$ ,  $a'_{1j} = 0$  pour  $j > 1$  et  $a'_{i1} = 0$  pour  $i > 1$ . Par l'utilisation répétée de cette étape de réduction,  $A$  est finalement transformé en une matrice diagonale où les éléments diagonaux sont non négatifs. Bien sûr lorsque nous effectuons des opérations sur les lignes et les colonnes de  $A$ , on obtient une suite de matrices de coefficients. Soit  $\mu$  la plus petite valeur absolue des éléments non nuls de la matrice actuelle. Localisons un élément de valeur absolue  $\mu$  dans, par exemple, une position  $(i_0, j_0)$ . Utilisons l'opération (C1) or (R1) pour réduire les autres coefficients dans la ligne  $i_0$  ou la colonne  $j_0$ . Cela donne lieu à une nouvelle matrice avec de nouveaux coefficients avec une valeur pour  $\mu$  strictement plus petit, sauf si tous les autres coefficients de la ligne  $i_0$  et de la colonne  $j_0$ . Puisque  $\mu$  ne peut prendre que des valeurs intégrales positives, cette dernière situation doit éventuellement se produire. Puis, nous utilisons les opérations (R2) et (C2) pour déplacer le coefficient de

la position  $(i_0, j_0)$  vers  $(1, 1)$ . Si le coefficient est négatif, nous utilisons (C3) pour inverser le signe. Chaque fois que nous appliquons une opération de colonne à la matrice de coefficients  $A$ , nous appliquons également la même opération de colonne à  $V$ , et chaque fois que nous appliquons une opération de ligne à  $A$ , nous appliquons la même opération de ligne à  $B$ . La procédure de réduction prendra fin une fois que dans la sous-matrice qui reste à traiter tous les éléments sont 0. Ainsi on obtient une matrice diagonale avec des éléments positives dans les  $r$  premières lignes et 0 ailleurs. On peut démontrer que  $r$  est le rang de la matrice  $A$  donnée initialement.

**Remarque 2.0.1** *Attention à toutes les étapes du processus de réduction, les opérations de la colonne doit impliquer uniquement les colonnes 1 à  $n$ . De même, les opérations sur les lignes doivent n'impliquer que les lignes 1 à  $m$ . Lorsqu'on arrive au système  $DY = B'$ , alors on sait tout sur (1) i.e. :*

- (a) Ne possède pas de solutions.
- (b) Il possède une solution unique.
- (c) Il possède une infinité de solutions.

Dans la suite nous illustrons cette méthode par plusieurs exemples.

**Exemple 2.0.2** *Résoudre l'équation suivante :  $903x + 731y = 2107$ .*

**Solution 2.0.2** *Rappel. L'équation  $ax + by = c$  a des solutions si et seulement si  $(a, b) | c$ . Dans notre cas  $(903, 731) = 43$  et 43 divise 2107 car  $2107 = 7^2 \times 43$ . Alors l'équation possède une infinité de solutions.  $903x + 731y = 2107$  équivaut à*

$$21x + 17y = 49$$

On a :

$$\begin{array}{ccc|ccc} 21 & 17 & 49 & & 4 & 17 & 49 & & 4 & 1 & 49 \\ 1 & 0 & & \sim & 1 & 0 & & \sim & 1 & -4 & \\ 0 & 1 & & & -1 & 1 & & & -1 & 5 & \end{array}$$

$$\begin{array}{ccc} 0 & 1 & 49 & 1 & 0 & 49 \\ \sim & 17 & -4 & \sim & -4 & 17 & . \\ & -21 & 5 & & 5 & -21 \end{array}$$

Alors  $t = 49$ . D'où  $x = -4t + 17v$ ,  $y = 5t - 21v$ . D'où

$$x = -196 + 17v, y = 245 - 21v$$

où  $v \in \mathbb{Z}$ .

**Exemple 2.0.3** Résoudre l'équation suivante  $2x + 3y + 4z = 5 \dots (1)$

**Solution 2.0.3** On  $(2, 3, 4) = 1$  et 1 divise 5. Donc l'équation (1) a des solutions dans  $\mathbb{Z}$ .

On a

$$\begin{array}{cccc} 2 & 3 & 4 & 5 & 2 & 1 & 0 & 5 & 0 & 1 & 0 & 5 \\ 1 & 0 & 0 & & 1 & -1 & -2 & & 3 & -1 & -2 & \\ & & & \sim & & & & \sim & & & & . \\ 0 & 1 & 0 & & 0 & 1 & 0 & & -2 & 1 & 0 & \\ 0 & 0 & 1 & & 0 & 0 & 1 & & 0 & 0 & 1 & \end{array}$$

On trouve  $u = 5$ ,  $x = 3t - 2v - 5$ ,  $y = -2t + 5$ ,  $z = v, v \in \mathbb{Z}$ .

**Exemple 2.0.4** Résoudre le système suivant

$$\begin{cases} 20x + 44y + 50z = 10 \\ 17x + 13y + 11z = 19 \end{cases}$$

**Solution 2.0.4** On a :

$$\begin{array}{cccc} 20 & 44 & 50 & 10 & -80 & -6 & 50 & 10 & -98 & -6 & 80 & 10 \\ 17 & 13 & 11 & 19 & -5 & 2 & 11 & 19 & 1 & 2 & 1 & 19 \\ 1 & 0 & 0 & & \rightarrow & 1 & 0 & 0 & \rightarrow & 1 & 0 & 0 \\ 0 & 1 & 0 & & & 0 & 1 & 0 & & 3 & 1 & -5 \\ 0 & 0 & 1 & & & -2 & -1 & 1 & & -5 & -1 & 6 \end{array}$$

$$\begin{array}{cccc|cccc|cccc}
 -98 & 190 & 178 & 1872 & 0 & 190 & 178 & 1872 & 1 & 0 & 0 & 19 \\
 1 & 0 & 0 & 19 & 1 & 0 & 0 & 19 & 0 & 12 & 178 & 1872 \\
 1 & -2 & -1 & & \rightarrow & 1 & -2 & -1 & \rightarrow & 1 & -1 & -1 \\
 3 & -5 & -8 & & & 3 & -5 & -8 & & 3 & 3 & -8 \\
 -5 & 9 & 11 & & & -5 & 9 & 11 & & -5 & -2 & 11
 \end{array}$$

$$\begin{array}{cccc|cccc|cccc}
 1 & 0 & 0 & 19 & 1 & 0 & 0 & 19 & 1 & 0 & 0 & 19 \\
 0 & 12 & -2 & 1872 & 0 & 0 & -2 & 1872 & 0 & 2 & 0 & 1872 \\
 \rightarrow & 1 & -1 & 14 & \rightarrow & 1 & 83 & 14 & \rightarrow & 1 & -14 & 83 \\
 3 & 3 & -53 & & & 3 & -315 & -53 & & 3 & -316 & -315 \\
 -5 & -2 & 41 & & & -5 & 244 & 41 & & -5 & -41 & 244
 \end{array}$$

$$\begin{array}{cccc|l}
 1 & 0 & 0 & 19 & \\
 0 & 2 & 0 & 1872 & t = 19, 2u = 1872, \text{ donc } t = 19, u = 936 \\
 1 & -14 & 83 & & \\
 3 & 53 & -316 & & x = t - 14u + 83v = 83v - 13085 \\
 -5 & -41 & 244 & & y = 3t + 53u - 315v = -315v + 49665 \\
 & & & & z = -5t - 41u + 244v = 244v - 38471
 \end{array}$$

**Exemple 2.0.5** Résoudre le système

$$\begin{cases} x + 2y - z = 6 \\ 2x + z = 10 \end{cases} .$$

**Solution 2.0.5**

$$\begin{pmatrix} 1 & 2 & -1 & 6 \\ 2 & 0 & 1 & 10 \\ 1 & 0 & 0 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 6 \\ 2 & -4 & 3 & 10 \\ 1 & -2 & 1 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix}.$$

En prenant  $a_{11} = 1$  comme pivot et on utilise  $C1$ .

$$\begin{pmatrix} 1 & 0 & 0 & 6 \\ 2 & -4 & 3 & 10 \\ 1 & -2 & 1 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & -4 & 3 & -2 \\ 1 & -2 & 1 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix}$$

En prenant l'élément de la première ligne et la première colonne comme pivot et on utilise  $R1$ .

$$\begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & -4 & 3 & -2 \\ 1 & -2 & 1 & \\ 0 & 1 & 0 & \\ 0 & 0 & 1 & \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & -1 & 3 & -2 \\ 1 & -1 & 1 & \\ 0 & 1 & 0 & \\ 0 & 1 & 1 & \end{pmatrix}$$

En prenant l'élément de la deuxième ligne et la troisième comme pivot et on utilise  $C1$ .

$$\begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & -1 & 3 & -2 \\ 1 & -1 & 1 & \\ 0 & 1 & 0 & \\ 0 & 1 & 1 & \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & 1 & 3 & -2 \\ 1 & 1 & 1 & \\ 0 & -1 & 0 & \\ 0 & -1 & 1 & \end{pmatrix}$$

par C3.

$$\begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & 1 & 3 & -2 \\ 1 & 1 & 1 & \\ 0 & -1 & 0 & \\ 0 & -1 & 1 & \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & -2 \\ 1 & 1 & -2 & \\ 0 & -1 & 3 & \\ 0 & -1 & 4 & \end{pmatrix}$$

En prenant l'élément de la deuxième ligne et la deuxième colonne comme pivot et on utilise

$$C1. \text{ D'où } t = 6, u = -2. \text{ Ceci implique } \begin{cases} x = t + u - 2v \\ y = -u + 3v \\ z = -u + 4v \end{cases} . \text{ Par conséquent}$$

$$\begin{cases} x = 4 - 2v \\ y = 2 + 3v \\ z = 2 + 4v \end{cases} .$$

**Exemple 2.0.6** : Résoudre le système de congruence suivant

$$\begin{aligned} 3x + 3z &\equiv 1 \pmod{5} \\ 4x - y + z &\equiv 3 \pmod{5}. \end{aligned}$$

On travaille modulo 5.

**Solution 2.0.6** On a

$$\begin{array}{ccccccccc} 3 & 0 & 3 & 1 & 1 & 3 & 1 & 0 & 1 & 3 & 0 & 2 & 1 & 0 & 0 & 3 & 1 & 0 & 0 & 3 \\ 4 & -1 & 1 & 3 & 0 & 0 & 1 & 3 & 0 & 0 & 1 & 3 & 0 & 3 & 1 & 2 & 0 & 1 & 0 & 2 \\ 1 & 0 & 0 & & \rightarrow & 1 & 0 & 0 & \rightarrow & 1 & 0 & 0 & \rightarrow & 0 & 0 & 1 & \rightarrow & 0 & 1 & 2 \\ 0 & 1 & 0 & & & 0 & 1 & 0 & & 0 & 1 & 0 & & 0 & 1 & 0 & & 0 & 0 & 1 \\ 0 & 0 & 1 & & & 0 & 0 & 1 & & 0 & 0 & 1 & & 1 & 0 & 0 & & 1 & 1 & 3 \end{array}$$

On trouve  $t \equiv 3 \pmod{5}$   $u \equiv 2 \pmod{5}$  . D'où

$$\begin{cases} x \equiv u + 2v \equiv 2 + 2v \pmod{5} \\ y \equiv v \pmod{5} \\ z \equiv t + u + 3v \equiv 3v \pmod{5} \end{cases} .$$

**Exemple 2.0.7** *Discuter suivants les valeurs des entiers  $a, b, c$ , les solutions du système*

**Solution 2.0.7**

$$\begin{cases} x + 2y - 3z = a \\ 2x + 6y - 11z = b \\ x - 2y + 7z = c \end{cases}$$

*Sous forme matricielle ce système s'écrit*

$$\begin{array}{cccccc} 1 & 2 & -3 & x & a \\ 2 & 6 & -11 & y & = & b \\ 1 & -2 & 7 & z & c \end{array} .$$

$$\text{Mettons } A = \begin{pmatrix} 1 & 2 & -3 \\ 2 & 6 & -11 \\ 1 & -2 & 7 \end{pmatrix}, X = \begin{pmatrix} a \\ b \\ c \end{pmatrix}, Y = \begin{pmatrix} a & -3 \\ b & -11 \\ c & 7 \end{pmatrix} \text{ et } Z = \begin{pmatrix} 1 & 2 & a \\ 2 & 6 & b \\ 1 & -2 & c \end{pmatrix} .$$

$$\text{Alors on a } \det A = 0, \det X = 20a - 8b - 4c, \det Y = 10b - 25a + 5c \text{ et } \det Z = 4b - 10a + 2c.$$

*Remarquons que*

$$\begin{cases} 20a - 8b - 4c = 4(5a - 2b - c) \\ 10b - 25a + 5c = -5(5a - 2b - c) \\ 4b - 10a + 2c = -2(5a - 2b - c) \end{cases} .$$

*Donc si  $5a - 2b - c \neq 0$ , le système n'admet pas de solutions et si  $5a - 2b - c = 0$ , le système admet une infinité de solution.*

*Illustration numérique*

Pour  $a = 3$ ,  $b = 1$  et  $c = 7$ , le système 
$$\begin{pmatrix} 1 & 2 & -3 \\ 2 & 6 & -11 \\ 1 & -2 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 7 \end{pmatrix}$$
 n'a pas de solution.

Pour  $a = 1$ ,  $b = 3$  et  $c = -1$ , le système 
$$\begin{pmatrix} 1 & 2 & -3 \\ 2 & 6 & -11 \\ 1 & -2 & 7 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ -1 \end{pmatrix}$$
 possède les solutions suivantes

Les solutions sont

$$x = -4t - 2$$

$$y = 5t + 3, t \in \mathbb{Z}$$

$$z = t$$

# Chapitre 3

## Méthodes élémentaires pour la résolution d'équations diophantiennes

### 3.1 Méthode de factorisation

Soit l'équation  $f(x_1, x_2, \dots, x_n) = a$  on écrit cette équation sous la forme factorisée

$f_1(x_1, x_2, \dots, x_n)f_2(x_1, x_2, \dots, x_n) \dots f_n(x_1, x_2, \dots, x_n) = a$ , où  $f_1, f_2, \dots, f_n \in Z[x_1, x_2, \dots, x_n]$ .

En utilisant la factorisation de  $a$  en facteurs premiers on aboutit au système suivant

$$\left\{ \begin{array}{l} f_1(x_1, x_2, \dots, x_n) = a_1 \\ \dots\dots\dots \\ f_n(x_1, x_2, \dots, x_n) = a_n \end{array} \right. .$$

Enfin en résolvant ce système on trouve toutes les solutions de l'équation proposée.

**Exemple 3.1.1** Résoudre l'équation suivante :  $28x^2 - 23xy - 8x - 15y^2 + 10y = 105$ .

**Solution 3.1.1** Pour factoriser le premier membre de cette équation on utilise la méthode des coefficients indéterminés.  $28x^2 - 23xy - 8x - 15y^2 + 10y = (ax + by + c)(dx + ey)$ . Par

comparaison on obtient les équations

$$ad = 28$$

$$ae + bd = -23$$

$$cd = -8$$

$$be = -15$$

$$ce = 10$$

dont les solutions sont

$$a = 7 \quad b = 3 \quad c = -2 \quad d = 4 \quad e = -5 .$$

D'où  $28x^2 - 23xy - 8x - 15y^2 + 10y = (7x + 3y - 2)(4x - 5y) = 105 = 3 \times 5 \times 7$ . Ceci nous donne les systèmes suivants :  $\left\{ \begin{array}{l} 7x + 3y - 2 = 15 \\ 4x - y = 7 \end{array} \right.$  ,  $\left\{ \begin{array}{l} 7x + 3y - 2 = 21 \\ 4x - y = 5 \end{array} \right.$  dont les solutions sont respectivement  $(x, y) = (2, 1)$ ,  $(x, y) = (2, 3)$ .

**Exemple 3.1.2** Résoudre en entiers positifs l'équation  $x^3 + 3y^2 + xy = 13$ .

**Solution 3.1.2** On a  $x^3 = 13 - 3y^2 - xy \geq 0$ . Donc  $x^3 \leq 13$ , on trouve  $x \in \{1, 2\}$ .

Pour  $x = 1$ , on trouve  $3y^2 + y = 12$  (Pas de solutions entières)

Pour  $x = 2$ , on trouve  $3y^2 + 2y = 5$ , ce qui implique que l'on a une seule solution entière  $y = 1$ . Finalement la solution est  $(x, y) = (2, 1)$ .

**Exemple 3.1.3** Résoudre dans  $\mathbb{Z}$  ,l'équation  $x^6 + 3x^3 + 1 = y^4$ .

**Solution 3.1.3** On pose  $t = x^3$ , donc on a l'équation d'inconnue  $t$  suivante :  $t^2 + 3t + 1 = y^4$ .

L'utilisation de la forme canonique de  $t^2 + 3t + 1$  nous donne

$$\left(t + \frac{3}{2}\right)^2 - \frac{9}{4} + 1 = \left(t + \frac{3}{2}\right)^2 - \frac{5}{4}.$$

Donc  $\left(t + \frac{3}{2}\right)^2 - \frac{5}{4} = y^4$ . Alors  $(2t + 3)^2 - 4y^4 = 5$ . Ceci implique

$$(2t + 3 + y^2)(2t + 3 - y^2) = 5.$$

Nous distinguons les systèmes suivants

$$a) \begin{cases} 2t + 3 + 2y^2 = 5 \\ 2t + 3 - 2y^2 = 1 \end{cases} \quad \text{où les solutions sont } \begin{cases} (t, y) = (0, 1) \\ (t, y) = (0, -1) \end{cases}, \text{ d'où les solutions de l'équa-}$$

$$\text{tion initiale sont } \begin{cases} (x, y) = (0, 1) \\ (x, y) = (0, -1) \end{cases}.$$

$$b) \begin{cases} 2t + 3 + 2y^2 = 1 \\ 2t + 3 - 2y^2 = 5 \end{cases} \quad \text{il n'a pas de solutions.}$$

$$c) \begin{cases} 2t + 3 + 2y^2 = -5 \\ 2t + 3 - 2y^2 = -1 \end{cases} \quad \text{il n'a pas de solutions.}$$

$$d) \begin{cases} 2t + 3 + 2y^2 = -1 \\ 2t + 3 - 2y^2 = -5 \end{cases} \quad \text{il n'a pas de solutions.}$$

## 3.2 Méthode des inégalités

Cette méthode consiste à restreindre l'intervalle dans lequel les variables varient.

**Exemple 3.2.1** Soit l'équation suivante :  $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{2}$  tel que  $0 < x \leq y \leq z$ .

1. Démontrer que  $3 \leq x \leq 6$ .

2. Montrer que si  $x = 3$  alors  $7 \leq y \leq 12$ .

3. Achever la solution.

**Solution 3.2.1** 1. On a  $\frac{1}{x} \geq \frac{1}{y} \geq \frac{1}{z}$ , d'où  $\frac{3}{x} \geq \frac{1}{2}$  et donc  $x \leq 6$ . D'autre part  $\frac{1}{y} + \frac{1}{z} = \frac{1}{2} - \frac{1}{x} = \frac{x-2}{2x}$ , alors  $x \geq 3$ . Finalement  $3 \leq x \leq 6$ .

2. On a pour  $x = 3$ .  $\frac{1}{y} + \frac{1}{z} = \frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ , donc  $\frac{1}{z} = \frac{1}{6} - \frac{1}{y} = \frac{y-6}{6y}$ , d'où  $y \geq 7$ .

Par analogie on trouve  $4 \leq z \leq 42$ .

3. Finalement les solutions sont comme dans le tableau

$x$	$y$	$z$	$x$	$y$	$z$
3	12	12	4	12	6
3	8	24	5	10	5
3	9	18	6	6	6
3	10	15	5	10	5
4	8	8			

**Exemple 3.2.2** Trouver les triplets  $(x, y, z)$  d'entiers positifs tels que

$$(x + y)^2 + 3x + y + 1 = z^2$$

**Solution 3.2.2** On a pour tout  $x, y$  positifs

$$(x + y)^2 \leq (x + y)^2 + 3x + y + 1 \leq (x + y + 2)^2.$$

Puisque

$$(x + y)^2 + 3x + y + 1 = z^2.$$

On a

$$(x + y)^2 + 3x + y + 1 = (x + y + 1)^2.$$

Après simplification  $x = y$ . On pose  $x = y = k$ , on trouve  $(2k)^2 + 4k + 1 = z^2$  ce qui donne  $z = 2k + 1$ . Par conséquent  $(k, k, 2k + 1)$  est la solution de l'équation donnée où  $k \in \mathbb{N}$ .

**Exemple 3.2.3** Trouver les entiers  $x, y$  tels que  $x^3 + y^3 = (x + y)^2$ .

**Solution 3.2.3** On a

$$(x + y)^2 - (x^3 + y^3) = (x + y)(x + y + xy - x^2 - y^2).$$

Alors

$$(x + y)(x + y + xy - x^2 - y^2) = 0$$

est équivalent à

$$\begin{cases} x + y = 0 \\ x^2 + y^2 - xy - x - y = 0 \end{cases} .$$

Donc

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

Alors les valeurs possibles de  $x$  et  $y$  sont comme dans le tableau suivant

$x, y$	0	1	2
0	(0, 0)	(0, 1)	(0, 2)
1	(1, 0)	(1, 1)	(1, 2)
2	(2, 0)	(2, 1)	(2, 2)

Posons  $g(x, y) = (x - y)^2 + (x - 1)^2 + (y - 1)^2$ , alors on a

$$g(2, 2) = 2$$

$$g(1, 0) = g(0, 1) = 2 .$$

$$g(2, 1) = g(1, 2) = 2$$

Ce qui signifie que les solutions sont  $(0, 1)$ ,  $(1, 0)$ ,  $(2, 1)$ ,  $(1, 2)$ ,  $(2, 2)$ .

**Exemple 3.2.4** Trouver les triplets strictement positifs  $(x, y, z)$  tels que  $xy + xz + yz - xyz = 2$ .

**Solution 3.2.4** On a  $xy + xz + yz = 2 + xyz > xyz$ , alors  $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} > 1$ . Si  $x \leq y \leq z$ , on a  $\frac{3}{x} > 1$ , d'où  $x < 3$ , on trouve  $x \in \{1, 2\}$ . Pour  $x = 1$ , on a  $y + z = 2$ , alors  $y = z = 1$ . pour  $x = 2$  on a  $(y - 2)(z - 2) = 2$ , d'où  $y = 3, z = 4$ . Finalement les solutions sont  $(1, 1, 1), (2, 3, 4)$  .

**Exemple 3.2.5** Trouver les entiers  $x, y$  tels que  $(x^2 - y^2)^2 = 1 + 16y$ .

**Solution 3.2.5** Pour  $y = 0$ , on trouve  $x = \pm 1$ . Pour  $y > 0$ , (parceque  $(x^2 - y^2)^2 \geq 0$ ). On a  $(x^2 - y^2)^2 \geq 1$ , d'où  $|x^2 - y^2| \geq 1$ . On déduit que  $|x| \geq |y| + 1$ , ou  $|x| \leq |y| - 1$ . Dans ce cas on trouve  $(x^2 - y^2) \geq (2y - 1)^2$ . En résolvant cette inéquation, on trouve  $y \leq 5$  ou  $y \in \{1, 2, 3, 4, 5\}$ . Alors nous distinguons pour  $y$  les valeurs suivantes

- a)  $y = 1$ , pas de solutions entières.
- b)  $y = 2$ , pas de solutions entières.
- c)  $y = 3$ , deux solutions  $x = 4, x = -4$ .
- d)  $y = 4$ , pas de solutions entières.
- e)  $y = 5$ , deux solutions  $x = 4, x = -4$ .

Finalement les solutions de l'équation proposée sont  $(\pm 1, 0), (\pm 4, 3), (\pm 4, 5)$ .

### 3.3 Méthode paramétrique

Soit l'équation diophantienne  $f(x_1, x_2, \dots, x_n) = 0$ . Dans des situations particulières on peut écrire

$$\begin{cases} x_1 = g_1(k_1, k_2, \dots, k_n) \\ \dots\dots\dots \\ x_n = g_n(x_1, x_2, \dots, x_n) \end{cases}$$

tels que  $k_1, k_2, \dots, k_n$  des entiers(paramètres).

**Exemple 3.3.1** Trouver les triplets  $(x, y, z)$  tels que :  $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$

**Solution 3.3.1** On a  $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$ , d'où  $z = \frac{xy}{x+y}$ . Posons  $(x, y) = d$ . Alors  $x = dm, y = dn, (m, n) = 1$  et donc  $\frac{d^2mn}{d(m+n)} = \frac{dmn}{m+n}$ . Donc  $m+n | dmn$ , mais  $(mn, m+n) = 1$ , donc  $m+n | d$ . On déduit que

$$z = kmn, x = km(m+n), y = kn(m+n).$$

D'où pour  $m = 5$ ,  $n = 2$ ,  $k = 3$  on aura  $x = 105$ ,  $y = 42$ ,  $z = 30$  et on vérifie facilement que

$$\frac{1}{105} + \frac{1}{42} = \frac{1}{30}.$$

### 3.4 Méthode arithmétique modulaire

Dans des situations on s'intéresse à utiliser la congruence par rapport à un entier choisi convenablement pour dire que cette équation ne possède pas de solutions entières. Dans le cas contraire un bon choix de l'entier de congruence (i.e. l'entier par rapport au quel on fait la congruence) permettra de résoudre le problème posé.

**Exemple 3.4.1** *Démontrer que l'équation suivante n'a pas de solutions entières.*  $x^2 + 7y^2 = 3$ .

**Solution 3.4.1** *On utilise la congruence modulo 7, on a  $x^2 \equiv 3 \pmod{7}$ . Comme  $x^2 \equiv 0, 1, 2, 4 \pmod{7}$ , donc il n'y a pas de solutions entières.*

**Exemple 3.4.2** *Montrer qu'il n'existe pas d'entiers de la forme  $8n + 7$ , qui est la somme de trois carrés.*

**Solution 3.4.2** *Considérons l'équation  $8n + 7 = a^2 + b^2 + c^2$ . Les carrés modulo 8 sont 0, 1 et 4 i.e. on a que les possibilités suivantes  $x^2 \equiv 0 \pmod{8}$ ,  $x^2 \equiv 1 \pmod{8}$  et  $x^2 \equiv 4 \pmod{8}$ . En utilisant toutes les combinaisons possibles, avec ces entiers, on ne trouve jamais 7. Donc l'équation proposée n'a pas de solutions entières.*

**Exemple 3.4.3** *Montrer que l'équation*

$$(x + 1)^2 + (x + 2)^2 + \dots + (x + 2001)^2 = y^2$$

*elle n'a pas de solutions entières.*

**Solution 3.4.3** Rappelons que l'on a  $(x + i)^2 = x^2 + 2xi + i^2$ . Donc

$$\sum_{i=1}^{2001} (x + i)^2 = \sum_{i=1}^{2001} x^2 + 2 \sum_{i=1}^{2001} xi + \sum_{i=1}^{2001} i^2.$$

Alors

$$\sum_{i=1}^{2001} (x + i)^2 = (2001)(1001)x^2 + 4006002x + 2672671001 = y^2.$$

Mais

$$2001 \equiv 0 \pmod{3}$$

$$4006002 \equiv 0 \pmod{3}$$

$$2672671001 \equiv 2 \pmod{3}.$$

Comme  $y^2 \equiv 0, 1 \pmod{3}$ , l'équation proposée n'a pas de solutions entières.

**Exemple 3.4.4** Résoudre l'équation :  $3^x + 3^y = 6^z$ .

**Solution 3.4.4** En divisant les deux membres de l'équation par  $3^z$ , on trouve  $3^{x-z} + 3^{y-z} = 2^z$ . On a les cas suivants

- 1) Si  $x = y$ , on a  $3^{y-z} = 2^{z-1}$ ,  $x = y = z = 1$ .
- 2) Si  $x = z$ , on a  $y - z = 1$  ou  $y - z = 0$ , donc  $x = y = z = 1$ , ou  $x = z = 2, y = 3$ .
- 3) Si  $x > 0$  et  $y > z$ , pas de solutions.
- 4) Si  $x > 0$  et  $y < z$ , pas de solutions.
- 5) Si  $x < z$  et  $y < x$ , pas de solutions.
- 6) Si  $x < z$  et  $y < x$ , pas de solutions.

Les solutions sont donc  $(1, 1, 1), (2, 3, 2)$ .

## 3.5 Méthode d'induction

Cette méthode est basée sur le raisonnement par récurrence.

**Exemple 3.5.1** Trouver les solutions de l'équation suivante  $x^2 + y^2 + z^2 = 75^n$ .

**Solution 3.5.1** Nous avons  $1^2 + 5^2 + 7^2 = 75^1$  et  $10^2 + 14^2 + 73^2 = 75^2$ . Définissons la suite  $(x_n, y_n, z_n)$   $n, n \geq 3$  comme suit

$$x_{n+2} = 75x_n, y_{n+2} = 75y_n, z_{n+2} = 75z_n.$$

Si  $x_k^2 + y_k^2 + z_k^2 = 75^k$ , alors

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = (75x_k)^2 + (75y_k)^2 + (75z_k)^2.$$

Donc

$$x_{k+2}^2 + y_{k+2}^2 + z_{k+2}^2 = 75^2 (x_k^2 + y_k^2 + z_k^2) = 75^{k+2}.$$

On a deux suites solutions pour  $n \geq 1$  :

$$(x_{2n-1}, y_{2n-1}, z_{2n-1}) = (1 \times 75^{n-1}, 5 \times 75^{n-1}, 7 \times 75^{n-1})$$

$$(x_{2n}, y_{2n}, z_{2n}) = (10 \times 75^n, 14 \times 75^n, 73 \times 75^n).$$

Alors

$$n = 2, x_3 = 75, y_3 = 375, z_3 = 525$$

$$75^2 + 375^2 + 525^2 = 75^3 = 421875$$

et

$$n = 2, x_4 = 750, y_4 = 1050, z_4 = 5475$$

$$750^2 + 1050^2 + 5475^2 = 31640625 = 75^4.$$

**Exemple 3.5.2** Montrer que pour tout  $n \geq 3$ , il existe des entiers impairs positifs tels que  $7x^2 + y^2 = 2^n$ .

**Solution 3.5.2** Pour  $n = 3$ , on a  $x_3 = y_3 = 1$  et pour  $n = 4$ , on a  $x_4 = 1, y_4 = 3$ . On pose  $7x_n^2 + y_n^2 = 2^n$ . On aura

$$7 \left( \frac{x_n + y_n}{2} \right)^2 + \left( \frac{7x_n - y_n}{2} \right)^2 = 2(7x_n^2 + y_n^2) = 2^{n+1}$$

et

$$7 \left( \frac{x_n - y_n}{2} \right)^2 + \left( \frac{7x_n + y_n}{2} \right)^2 = 2(7x_n^2 + y_n^2) = 2^{n+1}$$

Donc on a deux suites solutions

$$\begin{cases} x_{n+1} = \frac{x_n + y_n}{2}, y_{n+1} = \frac{7x_n - y_n}{2} \\ x_{n+1} = \frac{|x_n - y_n|}{2}, y_{n+1} = \frac{7x_n + y_n}{2} \end{cases}.$$

**Exemple 3.5.3** Prouver que pour tout entier  $n \geq 3$ , l'équation  $\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = 1$ , a des solutions positives distinctes.

**Solution 3.5.3** Pour  $n = 3$ , on a  $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$ . Remarquons que

$$\sum_{k=1}^{k=n-1} \frac{k}{(k+1)!} = \sum_{k=1}^{n-1} \frac{k+1-1}{(k+1)!} = \sum_{k=1}^{k=n-1} \left( \frac{1}{k!} - \frac{1}{(k+1)!} \right).$$

Donc  $\frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \frac{1}{n!}$ , d'où  $(\frac{2!}{1}, \frac{3!}{2}, \dots, \frac{n!}{n-1}, n!)$  sont des solutions de l'équation. On a d'autres solutions ; en effet  $\frac{1}{2} + \frac{1}{2^2} + \dots + \frac{1}{2^{n-2}} = 1 - \frac{1}{2^{n-2}}$  et

$$\frac{1}{2^{n-2}} = \frac{2^{n-2} + 1}{2^{n-2}(2^{n-2} + 1)} = \frac{1}{2^{n-2} + 1} + \frac{1}{2^{n-2}(2^{n-2} + 1)}.$$

Donc

$$\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^{n-2}} + \frac{1}{2^{n-2} + 1} + \frac{1}{2^{n-2}(2^{n-2} + 1)} = 1$$

i.e.  $(2, 2^2, \dots, 2^{n-2} + 1, 2^{n-2}(2^{n-2} + 1))$  sont solutions de l'équation.

### 3.6 Méthode de la descente infinie de Fermat

Soit  $P(n)$  une propriété dépendante de l'entier naturel  $n$ . On cherche à démontrer que  $P(n)$  est fausse pour tout  $n$ . Pour cela, on raisonne par l'absurde :

- On suppose que pour un certain entier  $n$ ,  $P(n)$  est vraie.
- On démontre par ailleurs que pour chaque entier naturel  $n$  pour lequel  $P(n)$  est vraie, il

existe un entier naturel  $m$  strictement inférieur à  $n$  pour lequel  $P(m)$  est également vraie.

On conclut donc que  $P(n)$  n'est jamais vraie, car la suite des entiers naturels vérifiant la propriété  $P$  ne peut pas être strictement décroissante et infinie.

**Exemple 3.6.1** Résoudre l'équation  $x^2 + y^2 + z^2 = 2xyz$ .

**Solution 3.6.1** La seule solution est la solution triviale  $x = y = z = 0$ . Remarquons que  $x, y, z$  ne sont pas tous impaires. Sinon  $x^2 + y^2 + z^2 - 2xyz = 0$  serait impaire. D'où  $2 \mid xyz$ . Alors  $x^2 + y^2 + z^2 = 2xyz$  est divisible par 4. Comme tout carré parfait est congruent à 0 ou 1 modulo 4,  $x, y, z$  doivent tous être pairs. Posons  $x = 2x_1, y = 2y_1, z = 2z_1$ . On a  $4x_1^2 + 4y_1^2 + 4z_1^2 = 16x_1y_1z_1$  ou  $x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1$ . Comme  $x_1^2 + y_1^2 + z_1^2$  est divisible par 4,  $x_1, y_1$  et  $z_1$  sont aussi tous des pairs. De nouveau en posant  $x_1 = 2x_2, y_1 = 2y_2, z_1 = 2z_2$  nous trouvons une autre équation qui est

$$x_2^2 + y_2^2 + z_2^2 = 8x_2y_2z_2.$$

et ainsi de suite. En général, si  $n \geq 1$ ,  $x_n^2 + y_n^2 + z_n^2 = 2^{n+1}x_ny_nz_n$  implique que  $x_n, y_n, z_n$  sont tous pairs. Donc nous pouvons écrire  $x_n = 2x_{n+1}, y_n = 2y_{n+1}, z_n = 2z_{n+1}$  et on aura

$$x_{n+1}^2 + y_{n+1}^2 + z_{n+1}^2 = 2^{n+2}x_{n+1}y_{n+1}z_{n+1}.$$

En étirant ce processus on aura une suite infinie décroissante  $x_1, x_2, x_3, \dots$  où  $x_i = 2x_{i+1}$ . D'où  $|x_1| > |x_2| > \dots$  et ceci contredit F.M.I.D. (Fermat's Method of Infinite descent).

# Chapitre 4

## Quelques autres types d'équations diophantiennes

### 4.1 Equation $x^2 + y^2 = z^2$

**Solution 4.1.1** On a pour tout entiers  $m, n$  :  $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$ . Donc  $x = m^2 - n^2$ ,  $y = 2mn$ ,  $z = m^2 + n^2$ . Pour  $m = 17, n = 11$ , on trouve

$$x = 168, y = 374, z = 410$$

$$168^2 + 374^2 = 168100 = 410^2.$$

### 4.2 Equation $x^2 + y^2 = z^4$

**Solution 4.2.1** On pose  $t = z^2$ , on a  $x = m^2 - n^2$ ,  $y = 2mn$ ,  $t = m^2 + n^2$ . D'autre part on a comme solution de l'équation  $m^2 + n^2 = z^2$ ,  $m = a^2 - b^2$ ,  $n = 2ab$ ,  $z = a^2 + b^2$ . Finalement

$$x = a^4 + b^4 - 6a^2b^2, y = 4ab(a^2 - b^2), z = a^2 + b^2.$$

Pour  $a = 23, b = 5 : x = 126716, y = 309120, z = 578$  et donc

$$126716^2 + 309120^2 = 111612119056 = 578^4.$$

### 4.3 Equation $x^2 + (3y)^2 = z^2$

**Solution 4.3.1** On utilise la méthode arithmétique et le théorème de Pythagore. Posons

$x = a^2 - b^2, 3y = 2ab, z = a^2 + b^2$ . Alors

$$\begin{cases} 3|2ab \\ (3, 2) = 1. \end{cases}$$

Donc d'après le lemme de Gauss, on a  $3|ab$ . On peut choisir  $[a = 3u, b = v]$ . Les solutions sont

$$\begin{cases} x = 9u^2 - v^2 \\ y = 2uv \\ z = 9u^2 + v^2 \end{cases} .$$

Pour vérification nous prenons des valeurs pour  $u, v$  :

$u$	$v$	$x$	$y$	$z$
1	1	8	2	10
3	2	77	12	85
5	4	209	40	241

### 4.4 Equation $(2x)^2 + y^4 = z^2$

**Solution 4.4.1** De la même façon on trouve  $x = 2mn(m^2 + n^2), y = m^2 - n^2, z = m^4 + 6m^2n^2 + n^4$  où  $m > n$  pour des solutions positives.

## 4.5 Equation $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$

**Solution 4.5.1** On peut écrire l'équation précédente sous la forme  $z^2(x^2 + y^2) = x^2y^2$ . Posons  $d = (x, y)$  alors  $x = da$ ,  $y = db$ . Donc  $z^2(a^2 + b^2) = d^2a^2b^2$ . Puisque  $(a, b) = 1$ , on a successivement  $(a^2, b^2) = 1$  et  $(a^2 + b^2, a^2b^2) = 1$ . Alors  $a^2b^2|z^2$ , d'où  $ab|z$ . On pose  $z = tab$ , on trouve  $t(a^2 + b^2) = d$ , alors  $a^2 + b^2 = \frac{d}{t} = k^2$ , d'où

$$\begin{cases} a = M(u^2 - v^2) \\ b = M(2uv) \end{cases}.$$

Les solutions de l'équation donnée sont de la forme

$$\begin{aligned} x &= t(u^2 + v^2)(u^2 - v^2) \\ y &= 2tuv(u^2 + v^2) \\ z &= 2tuv(u^2 - v^2) \end{aligned}$$

Pour vérification on a

$t$	$u$	$v$	$x$	$y$	$z$
2	5	3	1088	2040	960
11	7	2	26235	16324	13860
13	3	1	1040	780	624

## 4.6 Equation $x^2 + y^2 = z^3$

**Solution 4.6.1** On utilise les identités remarquables suivantes

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= (ac + bd)^2 + (ad - bc)^2 \\ (a^2 + b^2)(c^2 + d^2) &= (ac - bd)^2 + (ad + bc)^2 \end{aligned}$$

où  $a, b, c, d$  des entiers. On a aussi

$$\begin{aligned} (m^2 + n^2)^3 &= (m^2 + n^2)^2 (m^2 + n^2) \\ &= [(m^2 - n^2) + (2mn)^2] (m^2 + n^2) \\ &= (m^3 + mn^2)^2 + (m^2n + n^3)^2 \\ &= (m^3 - 3mn^2)^2 + (3m^2n - n^3)^2. \end{aligned}$$

Ainsi on obtient les solutions suivantes

$$\begin{cases} x = m^3 + mn^2, y = m^2n + n^3, z = m^2 + n^2 \\ x = m^3 - 3mn^2, y = 3m^2n - n^3, z = m^2 + n^2 \end{cases}.$$

Pour des valeurs numériques on a

$m$	$n$	$x$	$y$	$z$
3	2	39	26	13
3	2	-9	46	13

## 4.7 Equation $xz = y^2 + 1$

**Solution 4.7.1** Rappelons l'identité de Lagrange

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Si on pose

$$\begin{cases} x = a^2 + b^2, & z = c^2 + d^2 \\ y = ac + bd, & (ad - bc)^2 = 1 \end{cases}$$

Alors les solutions de l'équation donnée sont

$$\left\{ \begin{array}{l} x = a^2 + b^2 \\ y = ac + bd \\ z = c^2 + d^2 \\ |ad - bc| = 1 \end{array} \right.$$

avec  $a, b, c, d$  des entiers. Donnons des valeurs à  $a, b, c, d$

$a$	$b$	$c$	$d$	$x$	$y$	$z$
5	2	7	3	29	41	54
12	1	47	4	145	568	2225
25	37	2	3	1994	161	13

## 4.8 Equation $x^2 + y^2 = u^2 + v^2$

**Solution 4.8.1** En utilisant les identités précédentes on trouve  $x = mp + nq$ ,  $y = mq - np$ ,  $u = mp - nq$ ,  $v = mq + np$ . En donnant des valeurs numériques on trouve des valeurs pour  $x, y$  :

$m$	$n$	$p$	$q$	$x$	$y$	$u$	$v$
5	3	2	1	13	-1	7	11
7	2	5	11	57	67	13	87
13	5	1	3	28	34	-2	44

## 4.9 Equation $4^x + 18^y = 22^z$

**Solution 4.9.1** On va démontrer que cette équation admet une seule solution,  $(x, y, z) = (1, 1, 1)$ . On peut écrire l'équation précédente sous la forme  $2^{2x} + 2^y 3^{2y} = 2^z 11^z$ . On distingue les cas suivants

1)  $2x > y$ . Dans ce cas on a  $2^y (2^{2x-y} + 3^{2y}) = 2^z 11^z$ . Cette est vérifiée ssi  $y = z$ . Donc  $2^{2x-z} + 9^z = 11^z$ . On pose  $2x - z = t$  on aura  $2^t + 9^z = 11^z$  où la solution est unique

$(u, z) = (1, 1)$ . Donc  $(x, y, z) = (1, 1, 1)$ .

**2)**  $2x = y$ . On a  $2^y(1 + 3^{2y}) = 2^z 11^z$ . Donc  $1 + 3^{4x} = 2^{z-4x} 11^z$ . On a  $1 + 3^{4x} \equiv 1 + (-1)^x \pmod{10}$

$2^z 11^z \equiv 2^z \pmod{10}$ .

Si  $x = 0$ , on a  $4^0 + 18^0 = 22^z$  (impossible)

Si  $x = 1$ , on a  $4^1 + 18^2 = 328 = 22^z$  (impossible)

**3)**  $2x < y$ . On a  $2^{2x}(1 + 2^{y-2x} 3^{2y}) = 2^z 11^z$ . On trouve  $z = 2x$ , donc  $1 + 2^{y-z} \cdot 3^{2y} = 11^z$

On a  $11^z - 1 - 2^{y-z} 3^{2y} \equiv (2^z - 1) \pmod{2}$ .

$2^z - 1 \equiv 0 \pmod{2}$ , alors  $z = 0$ , on a  $x = 0$ .

On a  $1 + 18^y = 1$  (impossible).

Finalement la seule solution de cette équation est  $(1, 1, 1)$ .

## 4.10 Equation $(x + y + z)xyz = u^2$

**Solution 4.10.1** *Rappel (Formule de Héron) : Soit  $ABC$  un triangle et  $A$  son aire tel que  $AB = a, AC = b, BC = c$ . On a  $A = \sqrt{p(p-a)(p-b)(p-c)}$  avec  $2p = a + b + c$ . Si on pose  $a = y + z, b = x + z$  et  $c = x + y$ , on obtient l'équation  $(x + y + z)xyz = A^2$ . Nous avons*

$$\begin{cases} x = \frac{1}{2}(b + c - a) \\ y = \frac{1}{2}(a + c - b) \\ z = \frac{1}{2}(a + b - c) \end{cases} .$$

*Supposons que  $ABC$  est rectangle en  $A$ . Alors*

$$\begin{cases} x = \frac{1}{2}(b + c - a) \\ y = \frac{1}{2}(a + c - b) \\ z = \frac{1}{2}(a + b - c) \\ u = \frac{1}{2}ab \\ a^2 + b^2 = c^2 \end{cases} .$$

*Pour vérification*

<i>a</i>	<i>b</i>	<i>c</i>	<i>u</i>	<i>x</i>	<i>y</i>	<i>z</i>
3	4	5	6	3	2	1
12	5	13	30	3	10	2
12	9	15	54	6	9	3

## 4.11 Equation de Pell-Fermat

On va considérer, dans cette section, l'équation

$$x^2 - Dy^2 = 1.$$

où  $D$  est un entier positif.

Dans le livre intitulé [*Arithmetics*], **Diphantus** a donné la solution de l'équation considérée où  $D$  est un entier strictement positif qui n'est pas un carré parfait. La solution est  $x = 2m^2 + 1$ ,  $y = 2m$ , pour  $D = m^2 + 1$ .

Au 5<sup>ième</sup> siècle, le mathématicien hindou **Baudhyana** a donné la solution de l'équation  $x^2 - 2y^2 = 1$  qui est  $x = 577$ ,  $y = 488$ . en utilisant la fraction  $\frac{577}{408}$  comme approximation de  $\sqrt{2}$ .

Au 7<sup>ième</sup> siècle, le mathématicien **Brahmaqupta** a donné la solution de l'équation  $x^2 - 92y^2 = 1$  qui est  $x = 1151$ ,  $y = 120$ .

Le mathématicien hindou **Bhaskara** a donné la solution de l'équation  $x^2 - 61y^2 = 1$  qui est  $x = 1766319049$ ,  $y = 226153980$

En 1657 Fermat, en considérant  $D$  comme entier qui n'est pas un carré parfait, a remarqué que si  $(x, y)$  est une solution pour  $x^2 - Dy^2 = 1$ , alors  $(x^2 + D^2y^2, 2xy)$  est aussi une solution car

$$(x^2 - Dy^2)^2 = (x^2 + D^2y^2)^2 - (2xy)^2 D = 1.$$

Pour vérification

$x$	$y$	$x^2 + D^2y^2$	$2xy$
3	2	17	12
17	12	577	408
577	408	665587	470832

On sait que dans  $\mathbb{Z}[\sqrt{D}]$ , on a  $N(x + y\sqrt{D}) = N(x - y\sqrt{D})$ . Donc pour la résolution de l'équation  $x^2 - 2y^2 = 1$ , on a

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n, \quad x_n - y_n\sqrt{2} = (3 - 2\sqrt{2})^n, \quad n \in \mathbb{Z}.$$

On trouve

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

Pour  $n = 10$ , on trouve  $x_{10} = 22619537$ ,  $y_{10} = 1599428$  et  $22619537^2 - 2 \times 1599428^2 = 1$ .

### 4.11.1 Méthode générale de résolution

Si  $D$  est un entier qui n'est pas un carré parfait, alors l'équation  $x^2 - Dy^2 = 1$ , admet une infinité de solutions

$$\begin{aligned} x_{n+1} &= x_1x_n + Dy_1y_n \\ y_{n+1} &= y_1x_n + x_1y_n \end{aligned} \quad \text{où } x_n, y_n, D \in \mathbb{Z}.$$

**Exemple 4.11.1** Soit l'équation  $x^2 - 7y^2 = 1$

**Solution 4.11.1** Le couple  $(8, 3)$  est solution de cette équation, donc  $(x_1, y_1) = (8, 3)$ . Alors on a comme solutions

$$\begin{cases} x_{n+1} = 8x_n + 21y_n \\ y_{n+1} = 3x_n + 8y_n \end{cases}.$$

Voila quelques exemples

$$\begin{cases} x & 127 & 2024 & 32257 \\ y & 48 & 765 & 12192 \end{cases} .$$

**Remarque.** L'équation  $x^2 - 7y^2 = -1$ , n'a pas de solution car  $-1$  n'est pas un carré dans  $\mathbb{Z}/7\mathbb{Z}$  i.e. l'équation  $x^2 \equiv -1 \pmod{7}$  n'a pas de solutions dans  $\mathbb{Z}/7\mathbb{Z}$ .

#### 4.11.2 Equation $ax^2 - by^2 = 1$

On doit avoir  $(a, b) = 1$ , pour que cette équation soit solvable dans  $\mathbb{Z}$  et nous illustrons la méthode de résolution par un exemple.

**Exemple 4.11.2** Résoudre dans  $\mathbb{Z}$ , l'équation  $3x^2 - 2y^2 = 1$ .

**Solution 4.11.2**  $(x, y) = (1, 1)$ , est une solution. Posons  $x = u + av, y = u + bv, a, b, u, v \in \mathbb{Z}$ .

Alors

$$\begin{aligned} 3x^2 - 2y^2 &= 3(u + av)^2 - 2(u + bv)^2 \\ &= (3a^2 - 2b^2)v^2 + u^2 + 2uv(3a - 2b). \end{aligned}$$

Pour avoir une équation en fonction de  $u^2, v^2$  seulement on doit avoir  $3a - 2b = 0$ , on peut choisir  $a = 2, b = 3$ . Donc on a  $x = u + 2v, y = u + 3v$ .

D'où on obtient l'équation  $u^2 - 6v^2 = 1$  qui a  $(u, v) = (5, 2)$  comme solution.

Posons  $u_n + \sqrt{6}v_n = (5 + 2\sqrt{6})^n$ , donc  $u_{n+1} + \sqrt{6}v_{n+1} = (5 + 2\sqrt{6})^{n+1}$

On trouve après simplification  $u_{n+1} = 5u_n + 12v_n$  et  $v_{n+1} = 2u_n + 5v_n$ . On a  $u_n = 3x_n - 2y_n, v_n = -x_n + y_n$ . On trouve finalement

$$\begin{cases} x_{n+1} = 5x_n + 4y_n \\ y_{n+1} = 6x_n + 5y_n \end{cases}, (x_0, y_0) = (1, 1).$$

Pour vérification

$$\begin{cases} x & 9 & 89 & 881 \\ y & 11 & 109 & 1079 \end{cases} .$$

On peut trouver les solutions en fonction de  $n$  de la façon suivante :

$$\begin{cases} u_n + \sqrt{6}v_n = (5 + 2\sqrt{6})^n \\ u_n - \sqrt{6}v_n = (5 - 2\sqrt{6})^n \end{cases}$$

ceci implique

$$\begin{cases} u_n = \frac{1}{2} \left[ (5 + 2\sqrt{6})^n + (5 - 2\sqrt{6})^n \right] \\ v_n = \frac{1}{2\sqrt{6}} \left[ (5 + 2\sqrt{6})^n - (5 - 2\sqrt{6})^n \right] \end{cases} .$$

Puis on trouve  $x_n, y_n$ , en fonction de  $n$ .

**Exemple 4.11.3** Résoudre l'équation suivante  $x^2 - 6xy + y^2 = 1$

**Solution 4.11.3** On peut écrire cette équation de la façon suivante

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

Posons  $u = x - y, v = x + y$ , on a alors

$$2u^2 - v^2 = 1 \dots (*)$$

où on observe que  $(1, 1)$  est une solution pour cette équation. Les solutions de l'équation (\*)

sont

$$\begin{cases} u = -\frac{\sqrt{2}}{4} \left[ (1 + \sqrt{2})^{2n+1} - (1 - \sqrt{2})^{2n+1} \right] \\ v = -\frac{1}{2} \left[ (1 + \sqrt{2})^{2n+1} + (1 - \sqrt{2})^{2n+1} \right] \end{cases} .$$

Nous avons  $x = \frac{u + v}{2}, y = \frac{v - u}{2}$ . En remplaçant les valeurs de  $u, v$  on trouve les valeurs de

$x, y$ .

### 4.11.3 Application 1

**Exemple 4.11.4** Trouver les entiers naturels  $n$  tels que  $\frac{n(n+1)}{3}$  soit un carré parfait.

**Solution 4.11.4** Posons  $\frac{n(n+1)}{3} = y^2$ , on trouve  $n(n+1) = 3y^2$ . On écrit  $n(n+1)$  sous forme canonique  $n(n+1) = \left(n + \frac{1}{2}\right)^2 - \frac{1}{4}$ . D'où on a  $(2n+1)^2 - 12y^2 = 1$ , équation de Pell-Fermat. On trouve

$$2n+1 = \frac{1}{2} \left(7 + 4\sqrt{3}\right)^k + \frac{1}{2} \left(7 - 4\sqrt{3}\right)^k.$$

Alors

$$n = \frac{1}{4} \left(7 + 4\sqrt{3}\right)^k + \frac{1}{4} \left(7 - 4\sqrt{3}\right)^k - \frac{1}{2}, k \in \mathbb{N}.$$

Pour vérification

$k$	1	2	5	7	10
$n$	3	48	131043	25421763	6868959555

### 4.11.4 Application 2 :

**Exemple 4.11.5** Démontrer que si la différence de deux cubes consécutifs est  $n^2$ , alors  $2n-1$ , est un carré parfait.

**Solution 4.11.5** Pour tout entier naturel  $a$  on a  $(a+1)^3 - a^3 = 3a^2 + 3a + 1$ . Donc  $3a^2 + 3a + 1 = n^2$ . Alors  $a^2 + a + \frac{1}{3} = \frac{n^2}{3}$ , d'où  $\left(a + \frac{1}{2}\right)^2 - \frac{1}{4} + \frac{1}{3} = \frac{n^2}{3}$ . Nous trouvons après simplification  $4n^2 - 3(2a+1)^2 = 1$ . C'est l'équation de Pell-Fermat et donc la solution est

$$2a+1 = \left| -\frac{1}{2} \left(7 + 4\sqrt{3}\right)^k - \frac{1}{2} \left(7 - 4\sqrt{3}\right)^k - \frac{\sqrt{3}}{3} \left[ \left(7 + 4\sqrt{3}\right)^k - \left(7 - 4\sqrt{3}\right)^k \right] \right|.$$

En simplifiant on trouve  $a$

$$d = (a + 1)^3 - a^3.$$

$$k = 1 \qquad k = 3$$

$$a = 7 \qquad 1455$$

$$n^2 = 169 \qquad 6355441$$

$$2n - 1 = 25 = 5^2 \quad 2n - 1 = 5041 = 71^2$$

## Conclusion

Après cette étude de quelques équations diophantiennes et de quelques méthodes de leur résolution on a constaté que

a) Les notions de base de théorie élémentaire des nombres peut suffire pour faire des recherches dans ce domaine.

b) Les problèmes posés sont souvent simples (des équations de la forme  $f(x_1, x_2, \dots, x_n) = 0$ ).

c) pour chaque équation nous devons chercher des idées propres à elles. Cela signifie que la recherche dans ce domaine fait travailler la matière grise et nécessite beaucoup de réflexion.

Donc c'est un domaine agréable et prometteur pour ceux qui ont de la détermination et la volonté de travailler en équations diophantiennes.

# Bibliographie

- [1] Don Redmond, Number theory, An Introduction, Editions Library of congress cataloging-in-Publication Data,1996.
- [2] François Liret, Arithmétique cours et exercices corrigés, Dunod, 2011.
- [3] Ivan Niven, Herbert S.Zuckerman, Hugh L.Montgomery, An introduction to the Theory of numbers, Fifth edition.
- [4] Jean Marie, Problems in the classical numbers, Editions AMS,2004 .
- [5] Jozsef Sandor, Geometric Theorems, Diophantine Equations, and Arithmetic Functions, Editions Americain Research.
- [6] Kenneth H.Rosen, Elementary number theory and Its applications, fifth édition, Pearson Adison Wesley, 2005.
- [7] Robert D.Carmicheal, Diophantine Analysis, Editions ,John Wiley & sons,1915.
- [8] Seymour Lipschutz, Algebre Lineaire Cours et Problèmes, Série Schaum, Editions,1977.
- [9] Titu Andreescu, Dorin Andrica,Ion Cucureseu – An introduction to Diophantine Equations, Editions Birkhauser, 2010.
- [10] Titu Andreescu, Dorin Andrica – Quadratic Diophantine Equations, Editions Springer, 2015.

## خلاصة

لقد كشفنا في هذه المذكرة عن طريقة حل نظام الخطي الديوفنتي . بالإضافة إلى ذلك ، قدمنا بعض الطرق، تسمى الطرق الأولية، لحل معادلة ديوفانتية. يتم توضيح كل طريقة من خلال حل معادلة خطية واحدة على الأقل. أنهينا مذكرتنا من خلال حل بعض الأنواع الأخرى من المعادلات الديوفانتية. قد يكون محتوى هذا العمل، في رأينا ، مناسباً للمبتدئين الذين يرغبون في الشروع في هذا الفرع من الرياضيات.

## Résumé

Dans ce travail nous avons exposé la méthode de résolution d'un système linéaire diophantien. De plus nous avons présenté quelques méthodes, appelées méthodes élémentaires, de résolution d'équation diophantienne. Chaque méthode est illustrée par la résolution d'au moins une équation concrète. Nous avons terminé notre mémoire par la résolution de quelques autres types d'équations diophantiennes. Le contenu de ce mémoire peut, à notre avis, être convenable au débutant désirant se lancer dans cette branche de mathématiques.

## Abstract

In this memoir we have exposed the method of solving of a diophantine linear system. In addition, we have presented some methods, called elementary methods, of solving of a diophantine equation. Each method is illustrated by solving at least one concrete equation. We ended our memoir by solving some other types of diophantine equations. The content of this work may, in our opinion, be suitable for a beginner wishing to embark on this branch of mathematics.

