N° d'ordre :

N° de série :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de

la Recherche Scientifique

UNIVERSITÉ HAMMA LAKHDAR EL OUED

FACULTÉ DES SCIENCES EXACTES

Mémoire de fin d'étude

MASTER ACADEMIQUE

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Spécialité : Mathématiques fondamentales

Thème

Les m-uplets Diophantiens

Présenté par : Youmbai M.Taha

Medaci Maroua

Soutenu publiquement devant le jury composé de

Guedda Lamine	MCA	Président	Univ. El Oued
YOUMBAI Ahmed El Amine	MCB	Rapporteur	Univ. El Oued
Djedidi Yacine	MAA	Examinateur	Univ. El Oued

Année universitaire 2021 – 2022

Table des matières

Notations

$\overline{K}$	: Clôture algébrique d'un corps K.
$\mathbb{A}^n(K)$	: Espace Affine.
$\mathbb{P}^n(K)$	: Espace Projectif.
O	: Le point à l'infini $(0, 1, 0)$.
$E(\mathbb{Q})$	: Courbe elliptique définie sur $\mathbb{Q}$.
$cl(P)$	: Classe d'un point P.
$\Delta(E)$	: Discriminant de la courbe Elliptique E.
$dis(f)$	: Discriminant du polynôme f.
$x(P)$	: l'Abscisse du point P.

Introduction

Une équation diophantienne est une équation dont les coefficients et les solutions recherchées sont des nombres entiers ou rationnelles. Gauss disait " Leur charme particulier vient de la simplicité des énoncés jointe à la difficulté des preuves ". L'exemple le plus connu à l'appui de ce jugement est le théorème de Fermat-Wiles. D'autres, comme l'équation $au + bv = c$ (théorème de Bachet-Bézout), se résolvent plus facilement. La résolution de ces équations a amené au développement de puissants outils mathématiques. Le terme est aussi utilisé pour les équations à coefficients rationnels. Les questions de cette nature entrent dans une branche des mathématiques appelée arithmétique.

L'intérêt de la résolution de questions de cette nature réside rarement dans l'établissement d'un théorème clé pour les mathématiques, la physique ou les applications industrielles, même s'il existe des contre exemples comme la cryptologie, qui fait grand usage du petit théorème de Fermat. Leur analyse amène le développement d'outils mathématiques puissants dont l'usage dépasse le cadre de l'arithmétique. Les formes quadratiques sont à cet égard exemplaires. La richesse et la beauté formelle des techniques issues de la résolution d'équations diophantiennes fait de l'arithmétique la branche reine des mathématiques pour David Hilbert.

Ce type d'équation doit son nom au mathématicien grec Diophante d'Alexandrie, un mathématicien vivant à une date incertaine, probablement autour du IIIe siècle.

Il est l'auteur d'un traité, Arithmétiques, étudiant des questions de cette nature. Dans ce mémoire, nous nous intéressons en particulier à deux types d'équations Diophantiennes, à savoir les m-uplets Diophantiens et les courbes elliptiques. ce travail comporte deux parties :

La première est dédiée aux courbes elliptiques que nous utiliserons comme outil pour résoudre quelques équations dans la deuxième partie. La second partie traite des ensembles spéciaux appelés les m-uplets Diophantiens. Nous avant étudier ses ensembles et leurs extensions, divers techniques ont été utilisé pour résoudre les problèmes.

Chapitre 1

Préliminaires

Dans cette section, nous définitions brièvement les notions fondamentales des courbes algébriques en particulier les coniques et les cubiques non singulières, qui se trouvent dans [11, 10, 13, 14]. Ces dernières nous serons utile dans les chapitres qui suivent.

1.1 Les courbes algébriques

Soit K un corps, et $\overline{K}$ une cloture algébrique de K.

Définition 1. *Un n-espace affine sur K est l'ensemble des n-uples*

$$\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \{(a_1, a_2, ..., a_n) \in \overline{K}\}.$$

Les points K-rationels de $\mathbb{A}^n$ est l'ensemble

$$\mathbb{A}^n(K) = \{(a_1, a_2, ..., a_n) \in K\}.$$

Considerant maintenant le plan affine $\mathbb{A}^2$:

Définition 2. *Une courbe algébrique est l'ensemble des points du plan dont les coordonnées satisfont une equation algébrique $f(x, y) = 0$ de degré $n \geqslant 1$.*

Exemple 1.

1) Pour $n = 1$, $f(x, y) = a_1x + a_2y + a_3 = 0$ est l'équation d'une droite.

2) Pour $n = 2$ et f irréductible :

$$f(x, y) = a_1x^2 + a_2xy + a_3y^2 + a_4x + a_5y + a_6 = 0$$

est l'équation d'un cercle ou d'une conique selon la valeur des cœfficients a_i .

3) Pour $n = 3$ et f irréductible :

$$f(x, y) = a_1x^3+a_2x^2y+a_3xy^2+a_4y^3+a_5x^2+a_6xy+a_7y^2+a_8x+a_9y+a_{10} \quad (1.1)$$

est l'équation d'une cubique non dégénérée.

1.2 Les Coniques

Ce sont les courbes du second degré d'équation générale :

$$ax^2 + by^2 + cyx + dy + ex + f = 0,$$

tel que $(a, b, c) \neq (0, 0, 0)$.

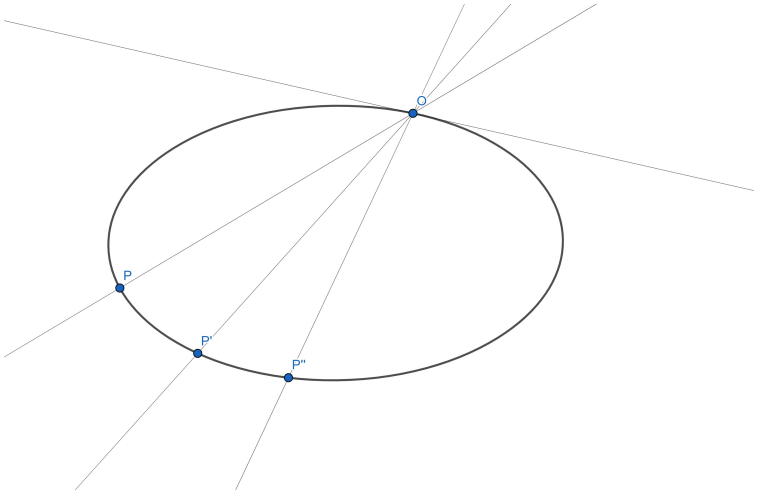
Exemple 2. *: Pour une conique d'équation $aX^2 + bY^2 = k$ et lorsque le produit $ab \neq 0$ (par exemple $a > 0$ et $b > 0$), trois cas peuvent être envisager.*

- $k = 0$ *La conique se réduit à* ***seul point rationnel****.*
- $k < 0$ *La conique ne possède* ***aucun point rationnel*** *.*
- $k > 0$ *La conique est* ***une ellipse*** *d'équation du type $\frac{X^2}{\alpha^2} + \frac{Y^2}{\beta^2} = 1$.*

1.2.1 Points rationnels sur une conique

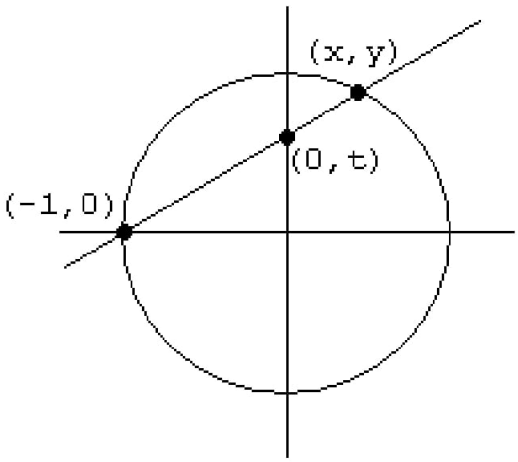
Une conique est dite rationnelle si le polynome dont elle est définie est à coefficients rationnels.

La connaissance d'un point rationnel de notre conique, disons O, permet de décrire les autres points rationnels de la conique. En effet, toute droite qui passe poar O coupe la conique en un deuxième point qui serait forcément a coordonnées rationnelles. On en déduit un isomorphisme entre les points d'une conique possèdant un point O et l'ensemble des droites passant par O.



Que donne ce procèdè dans le cas du cercle ?

Projetons le point $(-1, 0)$ sur l'axe des ordonnèes, dans la direction d'un certain point (x, y) du cercle.



On obtient un point $(0, t)$. L'équation de la droite que l'on vient de tracer est $y = t(1 + x)$. Mais si le point (x, y) est sur le cercle et sur cette droite, on obtient

l'équation :

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

Si t est fixé, cette équation de degré 2 en x a pour solution évidente -1 (par construction), l'autre solution s'obtient en simplifiant par $1 - x \neq 0$ ce qui donne $1 - x = t^2(1 + x)$, que l'on résout pour obtenir (sachant que $y = t(1 + x)$) :

$$x = \frac{1 - t^2}{1 + t^2} \quad et \quad y = \frac{2t}{1 + t^2}.$$

C'est une paramétrisation rationnelle du cercle car les coordonnées sont fractions rationnelles d'un paramètre. On voit sur ces formules que si t est rationnel, x et y sont des coordonnées d'un point rationnel du cercle. Réciproquement la formule $t = \frac{y}{1 + x}$ montre qu'un point rationnel du cercle est obtenu à partir d'un paramètre rationnel.

Les points rationnels du cercles sont donc exactement les points obtenus par les formules :
$x = \frac{1 - t^2}{1 + t^2} \quad et \quad y = \frac{2t}{1 + t^2}$, avec $t \in \mathbb{Q}$ (il faut ajouter le point $(-1, 0)$, qui s'obtient en prenant $t = \infty$).

On a donc résolu notre problème dans sa formulation géométrique puisqu'un triplet pythagoricien (a, b, c) est en relation avec les points rationnels du cercle par la formule $x = \frac{a}{c} \quad et \quad y = \frac{b}{c}$.

Chapitre 2

Les courbes elliptiques

Dans ce qui suit, nous présentons une études arithmétique et géométrique de base sur les courbes elliptiques, qui se trouvent principalement dans [10, 13, 14].

2.1 Singularités et genre d'une courbe algébrique lisse

Définition 3. *Un point $p = (x_p, y_p)$ d'une courbe algébrique C d'équation $f(x, y) = 0$ est singulier si ses coordonnées satisfont le système :*

$f(p) = f'_x(p) = f'_y(p) = 0$ *pour un point double,*

$f(p) = f'_x(p) = f'_y(p) = f''_{x^2}(p) = f''_{xy}(p) = f''_{y^2}(p) = 0$ *pour un point triple,*

$f(p) = f'_x(p) = \cdots = f^{n-1}_{x^{n-1}}(p) = f^{n-1}_{y^{n-1}}(p) = 0$ *pour un point multiple d'ordre n.*

Dans ces équations, les symboles f'_x, f'_y, désignent les dérivées partielles, $f^{(3)}_{x^3} = \dfrac{\partial^3 f}{\partial x^3}, \qquad f^{(3)}_{x^2y} = \dfrac{\partial^3 f}{\partial x^2 \partial y}$, etc...
Le degré n et le nombre s de points singuliers d'une courbe algébrique C sont associés à l'invariant « genre de la courbe ».

Définition 4. *Le genre d'une courbe algébrique C plane, irréductible, de degré $n \geqslant 2$ possédant s points singuliers, est l'entier non négatif :*

$g(c) = \frac{1}{2}(n-1)(n-2) - s.$

Exemple 3.

1) le genre d'une conique (C) *est égal à* $g(C) = 0$ *;*

2) le genre d'une cercle (C) *est égal à* $g(C) = 0$ *;*

3) le genre d'une cubique singulière (C) *est égal à* $g(C) = 0$ *;*

4) le genre d'une cubique (C) *non singulière est égal à* $g(C) = 1.$

2.2 Equation de Weierstrass d'une cubique irréductible

D'après la formule (1.1) précédente, l'équation d'une cubique plane, irréductible, dépend de dix cœfficients.
Il y a des équations particulières de cubiques irréductibles avec cinq cœfficients.

Définition 5. *L'équation de Weierstrass d'une cubique plane, irréductible* E *est de la forme :*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Cette équation est unitaire en y^2.
Des transformations linéaires de cette équation seront étudiées dans un autre paragraphe.

2.2.1 espaces projectifs :

Considérons un corps commutatif K et l'espace vectoriel K^n des points $a = (a_1, \ldots, a_n)$ à n coordonnés a_i dans K.
Soit $\mathbb{A}^n = \mathbb{A}^n(K) = \{a = (a_1, \ldots, a_n); a_1, \ldots, a_n \in K\}$ le n-espace affine de l'espace K^n :

Avec une relation d'équivalence sur un $n+1$ espace affine $\mathbb{A}^{n+1}$, nous construisons un espace projectif $\mathbb{P}^n$.

Définition 6. *Un espace projectif $\mathbb{P}^n(K)$ est l'espace quotient d'un $(n+1)$-espace affine $\mathbb{A}^n(k)$ par la relation d'équivalence T définie par :*
$a = (a_1, \ldots, a_{n+1})T(b_1, \ldots, b_{n+1}) = b$ *si et seulement si :*
$a = \lambda b$ *pour* $\lambda \neq 0$ *et* $\lambda \in k$.
$\mathbb{P}^n(K) = \mathbb{A}^{n+1}/T$.

Cette définition implique qu'un point P de l'espace projectif $\mathbb{P}^n$ admet $(n+1)$ coordonnées

$$P = (x_1, x_2, \ldots, x_{n+1}) \in \mathbb{P}^n.$$

Chaque point P est donc le représentant d'une classe :
$cl(p) = \{(x_1, x_2, \ldots, x_{n+1}), (yx_1, yx_2, \ldots, yx_{n+1}), (tx_1, tx_2, \ldots, tx_{n+1}), \ldots\}$.
Un point $P \in \mathbb{P}^n$ est parfois noté $(x_1 : x_2 : \ldots : x_{n+1}); x_1, x_2, \ldots x_{n+1}$ sont appelées les coordonnées homogènes de P.

Exemple 4. *dans l'espace projectif $\mathbb{P}^2(\mathbb{R})$, il y a une infinité de classes.*

$$cl(1,1,1) = \{(1,1,1), (-1,-1,-1), (2,2,2), \ldots\},$$
$$cl(0,0,1) = \{(0,0,1), (0,0,-1), (0,0,2), \ldots\},$$
$$cl(1,1,1) = \{(0,1,0), (0,-1,-0), (0,2,0), \ldots\}.$$

L'équation de Weierstrass d'une cubique E est de la forme :

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

C'est un polynôme homogène de 3 variables et de degré 3.
Dans un plan projectif $\mathbb{P}^n$, les polynômes sont homogènes à $n+1$ variables et de

degré $n \geqslant 1$.

La comparaison d'une équation de Weierstrass dans le plan affine $\mathbb{A}^2$ et dans le plan projectif $\mathbb{P}^2$ implique les formules de passage d'un plan à l'autre.

Le passage du plan projectif $\mathbb{P}^2$ au plan affine $\mathbb{A}^2$ s'obtient avec la transformation linéaire

$$(x, y, z) \longrightarrow (x, y, 1).$$

Le passage du plan affine $\mathbb{A}^2$ au plan projectif $\mathbb{P}^2$ s'obtient avec 2 opérations :

une transformation rationnelle

$$(x, y) \longrightarrow \left(\frac{x}{z}, \frac{y}{z}\right),$$

et une multiplication par z^d, $d =$ degré du polynôme f.

$$z^d f\left(\frac{x}{z}, \frac{y}{z}\right) = g(x, y, z).$$

Exemple 5.

1) $f(x, y, z) = 2x^5 - 3y^2x^3 + 4xyz^3 - 2z^5 \in \mathbb{P}^2$. *Ce polynôme homogène est transformé en un polynôme affine :*

   $f(x, y, 1) = g(x, y) = 2x^5 - 3y^2x^3 + 4xy - 2.$

2) *Le polynôme affine* $u(x, y) = x^4 - 2x^3y + x^2y + 5$ *est transformé en*

$$u\left(\frac{x}{z}, \frac{y}{z}\right) = \frac{x^4}{z^4} - 2\frac{x^3y}{z^4} + \frac{x^2y}{z^3} + 5$$

   puis, par multiplication par z^4, *en un polynôme homogène*

$$z^4 u\left(\frac{x}{z}, \frac{y}{z}\right) = x^4 - 2x^3y + x^2yz + 5z^4.$$

2.2.2 Transformation de l'équation de Weierstrass.

Par définition, l'équation de Weierstrass d'une cubique est de la forme :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6; \tag{1}$$

Pour éliminer certains monômes dans (1), il faut des transformations convenables :

Nous éliminons les monômes en xy et en y avec le changement de variables :

$$(x, y) \longrightarrow \left(X, \frac{1}{2}(Y - a_1X - a_3)\right). \tag{1-2}$$

Nous obtenons pour un corps K de carac $(K) \neq 2$, l'équation de Weierstrass :

$$E_1 : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6. \tag{1-3}$$

Les trois coefficients b_{2i} sont des polynômes homogènes de degré $2i$ ' de l'anneau $\mathbb{Z}[a_1, a_2, a_3, a_4, a_5, a_6]$:

$$b_2 = a_1^2 + 4a_2; \qquad b_4 = a_1a_3 + 2a_4; \qquad b_6 = a_3^2 + 4a_6. \tag{1-4}$$

L'élimination du coefficient 4 et du monôme en x^3 dans l'équation de E_1 s'obtient avec le changement de variables :

$$(X, Y) \longrightarrow \left(\frac{x - 3b_2}{36}, \frac{y}{108}\right); \tag{1-5}$$

Pour carac $(k) \neq 2, 3$, nous obtenons l'équation de Weierstrass :

$$E_2 : y^2 = x^3 - 27c_4x - 54c_6. \tag{1-6}$$

Les deux coefficients c_4 et c_6 sont des polynômes homogènes de degré $2i$ de l'anneau $\mathbb{Z}[b_2, b_4, b_6]$:

$$c_4 = b_2^2 - 24b_4; \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \tag{1-7}$$

Les deux changements de variables (1-2) et (1-5) sont des applications bijectives d'inverses :

$$(X, Y) \longrightarrow (x, 2y + a_1x + a_3); \quad et \quad (x, y) \longrightarrow (36X + 3b_2, 108Y). \tag{1-8}$$

Ces formules des b_{2i} et c_{2i} se trouvent dans [9], [13],[14]

D'autres transformations permettent d'obtenir d'autres modèles d'équations de Weierstrass :

Le modèle

$$E_3 : y^2 = x^3 + Ax + b. \tag{1-9}$$

Le modèle de Legendre :

$$E_4 : y^2 = x(x-1)(x-t), t \neq 0, 1.. \tag{1-10}$$

Le modèle de Kubert :

$$E_5 : y^2 + (1-c)xy - by = x^3 - bx^2. \tag{1-11}$$

Le modèle de During :

$$E_6 : y^2 + txy + ty = x^3, t \neq 27. \tag{1-12}$$

Le modèle de During :

$$E_7 : y^2 + xy = x^3 + ax + b \in \mathbb{A}^2(\mathbb{C}). \tag{1-13}$$

Selon Silvermane, les coefficients a et b sont des séries de puissances formelles dans l'anneau $\mathbb{Z}\big[[q]\big]$, $q = exp(2\pi iz)$.

$$a = -5\sum_{n\geqslant 1} n^3 q^n/(1-q^n),$$
$$b = -\frac{1}{12}\sum_{n\geqslant 1}(7n^5 + 5n^3)q^n/(1-q^n).$$

Signalons la transformation de l'équation de la courbe cubique de Fermat dans [16] page 201.

Equation de Fermat :

$$x^3 + y^3 = z^3 \qquad\qquad X = \frac{3z}{x+y} \quad , \qquad Y = \frac{9(x-y)}{2(x+y)} + \frac{1}{2}.$$

L'équation obtenue est de la forme :

$$Y^2 - Y = X^3 - 7.$$

Elle a pour invariants : $\delta(E) = -3^9, \quad j(E) = 0, \quad N(E) = 27.$

2.2.3 Discriminant d'une cubique

Les cubiques possèdent des invariants nombreux : géométriques, arithmétiques, algébriques, différentiels, analytiques ...

Nous nous intéressant par l'étude du discriminant pour classifier les cubiques

Définition 7. *Le discriminant d'une cubique d'équation de Weierstrass :*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

est le polynôme homogène de degré 12 *de l'anneau :* $\mathbb{Z}[b_2, b_4, b_6, b_8]$ *et égal à*

$$\delta(E) = 9b_2b_4b_6 - 8b_4^3 - 27b_6^2 - b_2^2b_8,$$

où l'on a posé $4b_8 = b_2b_6 - b_4^3$ *et pour carac* $(K) \neq 2, 3$.

2.2.4 Classification des cubiques planes

Considérons les cubiques planes E d'équation de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in \mathbf{K}[x, y]. \tag{1}$$

Lorsque le polynôme

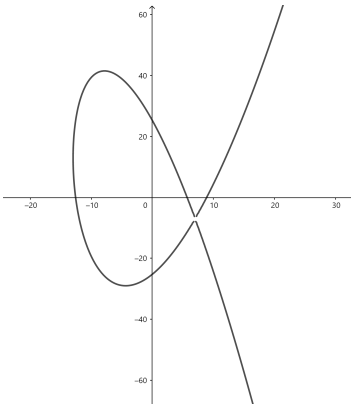
$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 \in \mathbf{K}[x, y] \tag{2}$$

est irréductible et sans point singulier, alors il est représenté par une courbe elliptique.

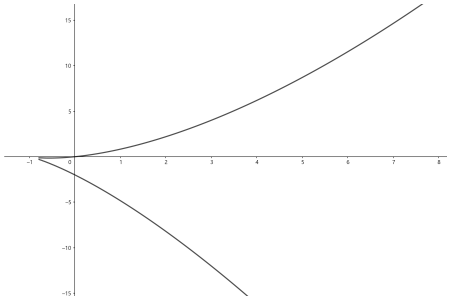
Définition 8. *Une courbe elliptique est une cubique irréductible, non singulière, qui a une équation de Weierstrass*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Dans le plan projectif $\mathbb{P}^2(K)$, une courbe elliptique a d'autres structures qui impliquent la possibilité d'autres définitions.
Une cubique E peut admettre 0 ou 1 point singulier. Le point singulier est soit un nœud, point singulier où la cubique E admet deux tangentes distinctes, soit un point de rebroussement, point singulier où la cubique admet deux tangentes confondues



$E : y^2 + 2xy = x^3 - 2x^2 - 133x + 637.$



$E : y^2 + 2xy + 2y = x^3 + 2x^2 + x.$

Proposition 1. *Soit une cubique E d'équation de Weierstrass projective :*

$$E : f(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0.$$

Le point $(0, 1, 0)$ à l'infini est un point simple de la cubique.

Démonstration. «Preuve de 0_E est un point de la cubique E »

Calculons la valeur $f(0_E)$; nous obtenons :

$f(0_E) = f(0, 1, 0) = 0.$

Il en résulte que le point 0_E est sur la cubique E.

Preuve de «0_E est un point simple E »

Calcul des trois dérivées partielles du polynôme f :

$$f_x^{'} = -3x^2 + a_1yz - 2a_2xz - a_4z^2, \tag{1}$$

$$f_y^{'} = 2yz + a_1xz + a_3z^2, \tag{2}$$

$$f_z^{'} = y^2 + a_1xy + 2a_3yz - a_2x^2 - a_4xz - 3a_6z^2. \tag{3}$$

La valeur $f_z^{'}(0_E) = f_z^{'}(0, 1, 0) = 1 \neq 0$ implique que le point 0_E est simple.

□

Etudions les cubiques singulières E avec leurs invariants $\Delta(E)$ et $c_4(E)$.

Proposition 2. *Soit une cubique de Weierstrass E, d'invariants $\Delta(E)$ et $c_4(E)$.*

1) la cubique est singulière si et seulement si $\Delta(E) = 0$.

2) elle admet un nœud si et seulement si $\Delta(E) = 0$ et $c_4(E) \neq 0$.

3) elle admet un point de rebroussement si et seulement si $\Delta(E) = 0$ et $c_4(E) = 0$.

Démonstration.

Preuve de «E est singulière» implique «$\Delta(E) = 0$» :

Par définition, une cubique singulière est une cubique E ayant un point singulier.

Donc ce point est double. (1)

L'équation de Weierstrass de la cubique est de la forme

$E : y^1 = (x-e)^2(x-e') = f(x); \quad s = (e, 0)$ est le point double. (2)

D'après la théorie des discriminants dis (f) de polynômes $f(x)$

dis $f(x) = 0$ si et seulement si f a une racine double. (3)

(2) et (3) impliquent dis $f(x) = 0$. (4)

La relation $\Delta(E) = 16\ dis(f)$ et (4) impliquent :

$\Delta(E) = 0.$ (5)

Preuve de «E admet un nœud» implique «$c_4(E) = 0$»

La cubique E admet deux tangentes distinctes au nœud. (6)

La pente d'une tangente à une courbe est égale à la dérivée y' de y.

Prenons une équation de Weierstrass de E de la forme :

$E : y^2 = x^3-27c_4x-54c_6.$ (7)

Calcul de la dérivée de y :

$$y' = \frac{3x^2 - 27c_4}{2y} = \frac{N(x)}{2y}. \quad (8)$$

L'hypothèse de deux tangentes distinctes au nœud implique :

Deux racines réelles distinctes du polynôme $N(x)$. (9)

Donc son discriminant dis $(N(x))$ n'est pas nul :

dis $(N(x)) = 12\times27c_4 \neq 0.$ (10)

Cela implique un invariant $c_4(E) \neq 0$.

Preuve de «E admet un point de rebroussement» implique «$\Delta(E) = 0$ etc $4(E) = 0$»

L'hypothèse « E admet un point de rebroussement » implique que la cubique est singulière, donc $$\Delta(E) = 0. \tag{11}$$

Gardons l'équation de Weierstrass (7) et la dérivée $y' \frac{N(x)}{2y}$. Au point de rebroussement, la cubique admet deux tangentes confondues, cela implique dis $(N(x)) = 0$;

D'après (10) : $$dis(N(x)) = 12 \times 27 c_4 = 0. \tag{12}$$

Il en résulte $$c_4(E) = 0. \tag{13}$$

□

Nous ne ferons pas la preuve des réciproques de (1), (2), (3).

Nous nous intéressons maintenant aux courbes elliptiques.

Proposition 3. *Soit une cubique de Weierstrass E de discriminant $\Delta(E)$*

1) la cubique E est une courbe elliptique si et seulement si $\Delta(E) \neq 0$.

2) La courbe elliptique E coupe l'axe Ox en trois points simples si et seulement si $\Delta > 0$.

3) La courbe elliptique E coupe l'axe Ox en un seul point si et seulement si $\Delta < 0$.

Démonstration. (1) d'après la proposition précédente, une cubique E est singulière si et seulement si $\Delta = 0$.

Il en résulte qu'une cubique est non singulière si et seulement si $\Delta(E) \neq 0$.

Par définition, une cubique non singulière est une courbe elliptique.

(2) Preuve de «une courbe elliptique E coupe l'axe Ox en 3 points simples implique $\Delta > 0$»

Considérons une courbe elliptique E qui coupe l'axe Ox en 3 points simples

$$p_i = (e_i, 0) : i = 1, 2, 3; \quad e_i \neq e_j. \tag{1}$$

Elle admet une équation de Weierstrass de la forme :

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) = f(x). \tag{2}$$

Le discriminant du polynôme $f(x)$ est égal à :

$$dis(f) = \prod_{1 \leqslant i < j \leqslant 3} (e_i - e_j)^2. \tag{3}$$

Les 3 racines e_i sont des nombres réels, il en résulte que les carrés $(e_i - e_j)^2$ de nombres réels sont positifs :

$$dis(f) > 0. \tag{4}$$

La formule (4) est la relation entre les discriminants de f et de E impliquent

$$\delta(E) > 0. \tag{5}$$

(3) Preuve de «une courbe elliptique coupe l'axe Ox en un seul point» implique «$\delta(E) < 0$».

Considérons une courbe elliptique qui coupe l'axe Ox en un seul point $P(e, 0)$.

Cela implique que les deux autres racines $e1$ et e_2 du polynôme $f(x) = y^2$ sont conjuguées complexes

$$e_1 = r + is, \quad e_2 = r - is \quad r \text{ et } s \text{ réels.} \tag{6}$$

Le discriminant du polynôme $f(x)$ est égal à

$$dis(f) = \big((e - e_1)(e - e_2)(e - e_3)\big)^2. \tag{7}$$

Avec le calcul nous obtenons la valeur :

$$dis(f) = -4s^2\big((e-r)^2 + s^2\big). \tag{8}$$

Les carrés des nombres réels sont positifs. Il en résulte que le signe du dis $f(x)$

$$dis(f) < 0. \tag{9}$$

La relation entre $dis(f)$ et $\delta(E) < 0$ implique :

$$\delta(E) < 0. \tag{10}$$

□

Nous ne ferons les preuves des réciproques.

En combinant les résultats des propositions (8) et (9), nous obtenons une classification des cubiques de Weierstrass par leurs invariants $\delta(E)$ et $c_4(E)$.

Corollaire 1. *Les cubiques E de Weierstrass sont classifiées par leurs invariants $\delta(E)$ et $c_4(E)$ en 4 classes.*

1) La classe $CubI$ des cubiques qui ont un nœud ; donc $\delta(E) = 0$ et $c_4(E) \neq 0$.

2) La classe $CubII$ des cubiques qui ont un point de rebroussement ; donc $\delta(E) = 0$ et $c_4 = 0$.

3) La classe $CubIII$ des courbes elliptiques qui coupent l'axe Ox en 3 points simples, donc $\delta(E) > 0$.

4) La classe $CubIV$ des courbes elliptiques qui coupent l'axe Ox en un seul point ; donc $\delta(E) < 0$.

Exemple 6.

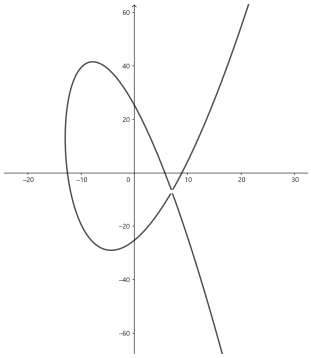
1) Cubique de Weierstrass qui a un nœud.

Cubique E_1 d'équation de Weierstrass :

$E_1 : y^2 + 2xy = x^3 - 2x^2 - 133x + 637.$

Calcul des invariants :

$\delta(E) = 0$ *et* $c_4 = 16 - 24(266) = -2^5.199 \neq 0.$



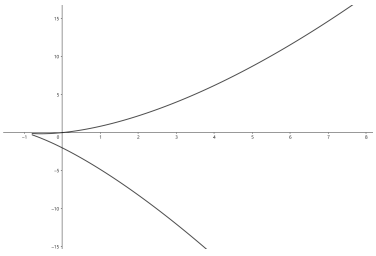
2) Cubique de Weierstrass qui a un point de rebroussement.

Cubique E_2 d'équation de Weierstrass :

$E_2 : y^2 + 2xy + 2y = x^3 + 2x^2 + x.$

Invariants :

$\delta(E_2) = 0$ *et* $c_4 = 0.$



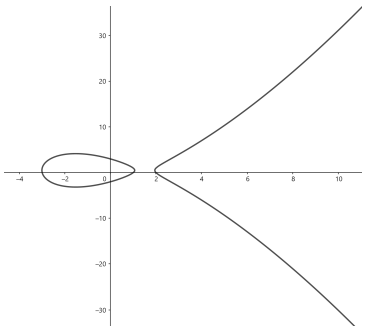
3) Courbe elliptique qui coupe l'axe Ox en 3 points simples.

Cubique E_3 d'équation de Weierstrass :

$E_3 : y^2 - y = x^3 - 7x + 6.$

d'invariant :

$\delta(E_3) = 5077 > 0.$



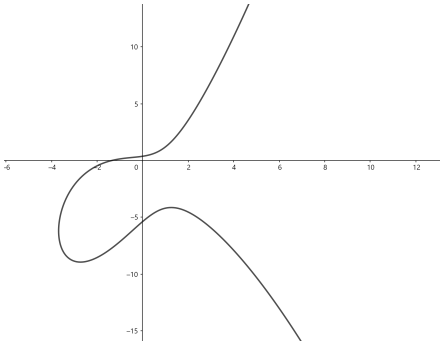
4) Courbe elliptique qui coupe l'axe Ox en un seul point.

Cubique E_4 d'équation de Weierstrass :

$E_4 : y^2 - 2xy + 5y = x^3 + x^2 + x + 2.$

d'invariant :

$\delta(E_4) = 64 - 27(33)^2 < 0.$



2.3 Groupe de Mordell-Weil

2.3.1 Loi de groupe :

Soient une cubique irréductible non singulière C et une droite L définies sur une clôture algébrique K de $\mathbb{Q}$.

Par le théorème de Bézout, si la cubique C a deux points d'intersection (comptés avec

leur multiplicité) avec la droite L, alors C a trois points d'intersection (comptés avec leur multiplicité) avec la droite L. Cela nous permet de définir une loi de composition.

Définition 9. ***(Loi de composition de la sécante-tangente)***
Soient P, Q deux points de $C(K)$, et L la droite passant par P et Q (la tangente en P si $P = Q$) et R le troisième point d'intersection de L avec C.
Soit L' la droite passant par R et O (point à l'infini). $P \oplus Q$ est défini comme étant le troisième point d'intersection de la droite L' avec C.

Cette loi munit $C(K)$ et $C(\mathbb{Q})$ d'une structure de groupes abéliens comme le montre la proposition suivante.

Proposition 4. *Cette loi de composition possède les propriétés suivantes :*

1) si L rencontre C en P, Q, R (non nécessairement distincts), alors

$$(P \oplus Q) \oplus R = 0.$$

2) $P \oplus O = P$ pour tout $P \in C$.

3) $P \oplus Q = Q \oplus P$ pour tout $P, Q \in C$.

4) Soit $P \in C$, alors il existe un point de C, qu'on note $(-P)$ tel que

$$P \oplus (-P) = O.$$

5) Soit P, Q et $R \in C$ alors

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

6) L'ensemble $C(K)$ est un groupe et $C(\mathbb{Q})$ est un sous groupe de $C(K)$.

Démonstration.

1) par définition de la loi de composition, (1) est trivial.

2) Posons $Q = O$, dans la définition de loi de composition, on voit que les droites L et L' (reliant $(P, Q = O)$ et (R, O) respectivement) coïncident.
L coupe C en P, O, R et L' coupe C en $R, O, P \oplus O$.
donc : $P = P \oplus O$.

3) Par construction cette loi est symétrique en P, Q d'où : $P \oplus Q = Q \oplus P$.

4) La droite reliant P et O, coupe C en un troisième point R. En utilisant (1) et (2) on a :

$$O = (P \oplus O) \oplus R = P \oplus R$$

.

5) En utilisant la formule donnant la somme de deux points P, Q donnée ci-après, un calcul laborieux que nous ne ferons pas, montre que la loi est associative. Mais nous donnons une autre démonstration de l'associativité basée sur la théorie des diviseurs.

6) Par ce qui précède, $C(K)$ est évidemment un groupe. Si les coordonnées de P, Q sont dans $\mathbb{Q}$, la droite reliant P et Q est à coefficients dans $\mathbb{Q}$, alors les coordonnées du troisième point d'intersection sont des combinaisons rationnelles des coordonnées de P et Q, et seraient donc dans $\mathbb{Q}$.
De la même manière si les coordonnées de P sont rationnels, les coordonnées de $(-P)$ le sont aussi.

□

2.3.2 Algorithme donnant la somme de deux points :

Soit une courbe elliptique E d'équation de Weierstrass

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Si $P_0 = (x_0, y_0)$ alors :

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3). \tag{1}$$

Soit maintenant P_1, P_2, P_3 tzls que $P_1 + P_2 = P_3$ avec $P_i = (x_i, y_i) \in E$:

Si $x_1 = x_2$ et $y_1 + y_2 + a_1x_2 + a_3 = 0$, alors

$$P_1 + P_2 = O. \tag{2}$$

Sinon, soit

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad v = \frac{y_1x_2 - y_2x_1}{x_2 - x_1} \quad \text{si} \quad x_1 \neq x_2, \tag{3}$$

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},\ v = \frac{-3x_1^2 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \quad \text{si}\, x_1 = x_2. \tag{4}$$

(Alors $y = \lambda x + v$ est la droite reliant P_1et P_2, ou tangente de E si $P_1 = P_2$).

$P_3 = P_1 + P_2$ est donné par

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - v - a_3.$$

Dans un cas spécial de (3), nous avons pour $P_1 \neq (\pm P_2)$

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

et la formule du double d'un point $P = (x, y) \in E$

$$x([2]P) = \frac{x^2 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4 + b_6},$$

où les b_i sont des polynômes en a_i, définis précédemment.

2.3.3 Théorème de Mordell-Weil :

Soit K un corps de nombre et E/K une courbe elliptique.

Mordell (1922), a montré qu'à partir d'un nombre fini de points K-rationnels du groupe de Mordell-Weil $E(K)$, on peut trouver tous les points K-rationnels de la courbe E.

En d'autre termes, il a montré le résultat suivant.

Théorème 1. *Le groupe $E(K)$ est de type fini.*

La preuve de ce fameux théorème se fait en deux parties distinctes.

1) *La première partie montre que pour $m \geqslant 2$, le quotient $E(K)/mE(K)$ est un groupe fini. La démonstration de sa finitude vient du fait qu'il s'injecte dans le groupe de Selmer d'une courbe elliptique qui est fini. Elle sera donnée plus loin, lors de l'étude des groupes de Selmer et de Tate-Shafarevitch.*

2) *La deuxième partie prend comme hypothèse $E(K)/mE(K)$ fini et prouve le théorème de Mordell-Weil en utilisant la procédure de la descente.*

Chapitre 3

Les m-uplets Diophantiens

Dans ce chapitre, nous introduisons les m-uplets Diophantiens, illustré par des exemples qui permettrons au lecteur de mieux comprendre cet notion. La plupart des travaux a ce sujet sont dûs a Andrey Dujella, qui a étudié minutieusement les m-uplets Diophantiens [3, 4, 5, 6], il sera donc notre référence de base.

Définition 10. *Un ensemble à m entiers positifs $a_1, a_2, \ldots, a_m$ est appelé un m-uplet Diophantien si, $a_i a_j + 1$ est un carré parfait pour $1 \leq i < j \leq m$.*

Le premier ensemble en nombres rationnels fut découvert par Diophante est :

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}.$$

3.1 Cas d'une pair Diophantienne

Un ensemble d'entiers positifs distincts $\{a, b\}$ est une paire Diophantienne si $ab+1$ est un carrè parfait.

Gènèralement, pour chaque entier $k \geqslant 2$ l'ensemble $\{k-1, k+1\}$ possède cette propriété et on peut facilement vèrifier que $(k-1)(k+1)+1 = k^2$.

3.2 Cas d'un triplet Diophantien

Supposons maintenant qu'on a une paire Diophantienne rationnelle $\{a, b\}$, l'extention de cette dérnière en un triplet Diophantien rationnel $\{a, b, c\}$ peut se faire avec des méthodes élémentaire. Il s'agit de résoudre le system

$$S = \begin{cases} ac + 1 = s^2 \dots (1) \\ bc + 1 = t^2 \dots (2) \end{cases}$$

Proposition 5. *Le system S est vérifié pour le rationnel*

$$c = \frac{4k(b - ak)(k - 1)}{(b - ak^2)^2} \qquad où \quad k \in \mathbb{Q}.$$

Démonstration. Multiplions l'équation (1) par b et l'équation (2) par a puis, faisons la différence, on obtient la conique d'équation :

$$bs^2 - at^2 = b - a.$$

Puisque elle possède la solution $(s, t) = (1, 1)$, on en déduit qu'il y est une infinité de solutions rationnelles.
En effet, on posant $s = s' + 1$ et $t = s'k + 1$ nous obtenons $s' = \dfrac{2ak - 2b}{b - ak^2}$, d'où :

$$s = \frac{b + ak^2 - 2ak}{ak^2 - b}.$$

Finalement, en remplaçant s dans (1) nous obtenons c.

□

Dans ce qui suit, nous utilisons la théorie des courbes elliptiques pour passer d'un triplet Diophantien à un quadruplet Diophantien.

3.3 Cas d'un Quadruple Diophantien

Soit $\{a, b, c\}$ un triplet Diophantien (rationnel), $c - a - d$

$$ab + 1 = r^2, \quad ac + 1 = s^2 \text{ et } \quad bc + 1 = t^2.$$

Afin de prolonger ce triplet en un quadruple $\{a, b, c, x\}$, il faut résoudre le système suivant :

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{3.1}$$

Définissons

$$d_+ = a + b + c + 2acb + 2rst, \qquad d_- = a + b + c + 2acb - 2rst.$$

On peut facilement vérifié que d_+ et d_- sont des solutions du Sys (3.1). En effet,

$$\begin{aligned}
ad_+ + 1 &= (at + rs)^2, \\
bd_+ + 1 &= (bs + rt)^2, \\
cd_+ + 1 &= (cr + st)^2, \\
ad_- + 1 &= (at - rs)^2, \\
bd_- + 1 &= (bs - rt)^2, \\
cd_- + 1 &= (cr - st)^2.
\end{aligned}$$

Notons que si a, b, c sont des entiers positifs, il y a une conjecture qui affirme que :

Conjecture 1. *Si x est un entier positif tel que a, b, c, x est un quadruple Diophantien, alors $x = d_+$ ou $x = d_-$.*

Pour trouver une solution rationelle, Il serait naturel d'attribuer au Sys (3.1) la courbe elliptique E d'équation

$$E : \qquad y^2 = (ax + 1)(bx + 1)(cx + 1). \tag{3.2}$$

Via le changement de variables bi-rationnels

$$x \mapsto \frac{X}{abc}, \qquad y \mapsto \frac{Y}{abc}.$$

L'équation de la courbe E conduit à une courbe elliptique équivalente d'équation

$$E' : \qquad Y^2 = (X + bc)(X + ac)(X + ab). \tag{3.3}$$

Le but de cette partie est d'étudier les relations entre les solutions du système (3.1) et l'équation (3.3).

Mentionnons que le système (3.1) où a, b, c sont des entiers rationels (arbitraires) est appelée le triplet d'équation de Fermat. Dans le cas général certains connexions entre (3.1) et (3.2) ont été étudiées dans [9, 12, 15].

La courbe (3.3) possède une infinité de solutions. Nous cherchons parmi ces dernières c'elles qui vérifient aussi le Sys (3.1).

Nous distinguons facilement les trois points rationnels sur E :

$$A = (-\frac{1}{a}, 0), \quad B = (-\frac{1}{b}, 0), \quad C = (-\frac{1}{c}, 0).$$

On a aussi D'autres points rationnels évidents comme :

$$P = (0, 1), \quad S = \left(\frac{1}{abc}, \frac{rst}{abc}\right).$$

Ce n'est pas si évident, mais il est facile de vérifier que $S \in 2E(\mathbb{Q})$. À savoir, $S = 2R$ où

$$R = \left(\frac{rs + rt + st + 1}{abc}, \frac{(r + s)(r + t)(s + t)}{abc}\right) \in E(\mathbb{Q}).$$

La répence de ce problème ce résume dans le théorème suivant :

Théorème 2. *Le point $T = (x_0, y_0) \in E$ tel que x_0 soit une solution de Sys (3.1) doit vérifié la condition*

$$T - P \in 2E(\mathbb{Q}).$$

3.3.1 Calcul Numérique

Soit $\{1, 3, 8\}$ un triplet Diophantien appelé Triplet de Fermat (nous allons voir plus loin comment obtenir ce triplet). Nous cherchons à étendre ce triplet en un

quadruplet Diophantien $\{1, 3, 8, x\}$, pour cela nous devons résoudre le système suivant :

$$S = \begin{cases} x + 1 = r^2, \\ 3x + 1 = s^2, \\ 8x + 1 = t^2. \end{cases} \tag{3.4}$$

Ce système peux être attribuer à la courbe elliptique

$$E : \qquad y^2 = (x + 1)(3x + 1)(8x + 1).$$

Via le changement de variables bi-rationnels

$$x \mapsto \frac{X}{24}, \qquad y \mapsto \frac{Y}{24}. \tag{3.5}$$

L'équation de la courbe E conduit à une courbe elliptique équivalente d'équation

$$E' : Y^2 = (X + 3)(X + 8)(X + 24).$$

Donc

$$P = (0, 1) \in E \longrightarrow P' = (0, 24) \in E'$$

et

$$T = (x_0, y_0) \in E \longrightarrow T' = (24x_0, 24y_0) \in E'.$$

Selon le Th.(2), une solution de Sys.(3.4) s'obtient par l'abscisse d'un point $T = (x_0, y_0)$ de la courbe E vérifiant la condition $T - P_E \in 2E$. Il suffit donc de trouver un point de E, calculer son double et lui ajouter le point $P = (0, 1)$.

On a, la courbe elliptique E' est engendrée par un seul élément $P' = (0, 24)$ selon le calcul par le logiciel Magma [2].

Remarque 1. *Comme P' est l'unique générateur de E', la courbe E est engendré par le point $p = (0, 1)$ qui correspond a P' d'après les transformations (3.5).*

Donc $E' \simeq E_{torsion} \times \mathbb{Z}^1$ et l'ensemble $(2n+1)P'$ vérifiant

$$(2n+1)P' - P' = 2nP' \in 2E'(\mathbb{Q}).$$

Donc une solution de Sys.(3.4) s'obtient par $\dfrac{x([2n+1]P')}{24}$.

Par exemple, sur certains points

$$3P_E = (120, 6479),$$
$$5P_E = \left(\frac{18659520}{8288641 \times 24}, \frac{897051404184}{23862997439 \times 24}\right),$$
$$9P_E = \left(\frac{256675231488887352993478 40}{828778442690908337472 1 \times 24}, \frac{434424747047482095147474558591556 2216}{754497263924870425140991078451519 \times 24}\right).$$

3.4 Cas d'un quintuple Diophantien

Soit $\{a, b, c, d\}$ un Quadruple Diophantien (rationnel), $c - a - d$

$$ab + 1 = r^2, \qquad ad + 1 = t^2, \qquad bd + 1 = v^2,$$
$$ac + 1 = s^2, \qquad bc + 1 = u^2, \qquad cd + 1 = w^2.$$

Pour étendre un Quadruple à un quintuple, il faut résoudre le système :

$$ax + 1 = \square, \quad bx + 1 = \square, \quad cx + 1 = \square, \quad dx + 1 = \square. \tag{3.6}$$

C'est une idée naturelle d'attribuer le système (3.6) la courbe elliptique

$$y^2 = (ax + 1)(bx + 1)(cx + 1)(dx + 1).$$

Par le changement de variables rationnel

$$t = \frac{y(d-a)(d-b)(d-c)}{(dx+1)^2}, \quad s = \frac{(ax+1)(d-b)(d-c)}{dx+1}$$

on obtient la courbe elliptique suivante

$$E: \quad t^2 = s(s+(b-c)(d-c))(s+(c-a)(d-b)). \tag{3.7}$$

Nous avons trois points de 2-torsions rationnels non triviaux sur E :

$$A = (0,0), \quad B = (-(b-a)(d-c),0), \quad C = (-(c-a)(d-b),0),$$

et deux autres points rationnels évidents :

$P = ((b-a)(c-a),(b-a)(c-a)(d-a))$,

$Q = ((ad+1)(bc+1), rstuvw)$.

$$e = \frac{\left((a+b+c+d)(abcd+1)+2abc+2abd+2acd+2bcd \pm 2rstuvw\right)}{(abcd-1)^2}.$$

Il été prouvé que $ae+1$, $be+1$, $ce+1$ et $de+1$ sont des carrés parfaits.

Par exemple $ae+1 = \dfrac{(auvw \pm rst)^2}{(abcd-1)^2}$.

Le point de départ est la famill $\{x, x+2, 4x+4\}$ qui constitue une famille infinie de 3-uplets Diophantiens. En posant, $\{a_1, a_2, a_3\} = \{x, x+2, 4x+4\}$,

$$x(x+2)+1 = (x+1)^2,$$

$$x(4x+4)+1 = (2x+1)^2,$$

$$(x+2)(4x+4)+1 = (2x+3)^2.$$

Puis,il rajoute $a_4 = 9x+6$, qui vérifie :

$$x(9x+6)+1 = (3x+1)^2,$$

$$(4x+4)(9x+6)+1=(6x+5)^2.$$

Il ne lui restait qu'à chercher une valeur positive de x telle que

$$(x+2)(9x+6)+1=\square.$$

En d'autres termes

$$9x^2+24x+13=\square,$$

$$(3x+4)^2-3=\square.$$

Pour ce faire, il posa $\square=(3x-4)^2$ et il trouva enfin :

$$x=\frac{1}{16}.$$

Pour trouver un quadruplet d'entiers positifs, Fermat, démarra du triplet $\{1,3,8\}$, en posant $x=1$, auquel il rajouta un quatrième élément d.

En considérant le système d'équations :

$$\begin{cases} d+1=\square, \\ 3d+1=\square, \\ 8d+1=\square. \end{cases}$$

et en posant $d=x^2-1$, il trouva le système :

$$\begin{cases} 3x^2-2=\square, \\ 8x^2-7=\square. \end{cases}$$

qui admet $x=11$ comme solution évidente, d'ou le premier quadruplet d'entiers :

$$\{1,3,8,120\}.$$

Depuis, une des questions s'est posée : Est-il possible d'étendre l'ensemble de Fermat $\{1, 3, 8, 120\}$ à un quintuplet d'entiers positifs ?

La réponse est négative, elle fut donnée par Baker et Davenport en 1969 [1].

En fait, l'ensemble de Fermat n'est qu'un exemple de la famille infinie de quadruplets

$$\left\{k-1, k+1, 4k, 16k^3-4k\right\},$$

prouvée non extensible à une famille de quintuplets, par A.Dujella, en 1997 [4].

A.Dujella prouva, de plus, que la famille de quadruplets $\left\{k-1, k+1, 4k, 16k^3-4k\right\}$ est la seule extension de $\{k-1, k+1, 4k\}$.

En 1998, A.Dujella et Petho [6], ont prouvé que l'ensemble $\{1, 3\}$ ne peut s'étendre à un quintuplet.

Un résultat plus général fut démontré par Fujita [7] en 2008, il stipule que l'ensemble $\{k-1, k+1\}$ est non extensible à un quintuplet.

Bien sur, Euler fut le premier à avoir essayé, de répondre à la question.Il commenca par généraliser la famille des quadruplets diophantiens, en montrant simlement le résultat suivant :

Si $\{a, b\}$ est un 2-uplet diophantien, alors :

$$\left\{a, b, a+b+2r, 4r(r+a)(r+b)\right\}, r=\sqrt{ab+1}$$

est un quadruplet diophantien.

Il est clair que si $a = k-1$ et $b = k+1$, on retrouve la famille $\left\{k-1, k+1, 4k, 16k^3-4k\right\}$ qui ne contient pas, par exemple, le quadruplet diophantine $\{2, 12, 24, 2380\}$, correspondant à $r = 5$.

Il proposa enfin une extension du quadruplet de Fermat à un cinquième élément mais

dans $\mathbb{Q}^+$:

$$\left\{1, 3, 8, 120, \frac{777480}{8288641}\right\}.$$

En 2006, Gibbs [8] a pu trouver un sextuplet dans $\mathbb{Q}^+$:

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}.$$

Bibliographie

[1] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Quart.J.Math. Oxford Ser.(2) 20 (1969), 129-137.

[2] W. Bosma, J.J. Cannon, C. Fieker and A. Steel (eds.), Handbook of Magma functions, Edition 2.20-9, 2014.

[3] A. Dujella, "Diophantine m-tuples and elliptic curves." Journal de théorie des nombres de Bordeaux 13.1 (2001) : 111-124.

[4] A. Dujella, on Diophantine quintuples, Acta Arith. 81 (1997), 69-79.

[5] A. Dujella, "Irregular Diophantine m-tuples and elliptic curves of high rank." Proceedings of the Japan Academy, Series A, Mathematical Sciences 76.5 (2000) : 66-67.

[6] A. Dujella and A. Pethoe, A generalization of a theorem of Baker and Davenport, Quart. J. Math. Oxford ser. (2), 49 (1998), 291-306.

[7] Fujita, The number of $D(-1)$-quadruples. Math. Commun. 15, 387-391 (2010) 12.

[8] P Gibbs, Some rational Diophantine sextuples, Glas. Mat. Ser. III 41(2006), 195-203.

[9] E. HERRMANN, A. PETHÖ, H.G. ZIMMER, On Fermat's quadruple equations. Abh. Math. Sem. Univ. Hamburg 69 (1999), 283-291.

[10] D. HUSEMÖLLER, Elliptic Curves. Springer-Verlag, New York, 1987.

[11] D. Perrin, (2013). Géométrie algébrique. Edp Sciences.

[12] A. PETHÖ, E. HERRMANN, H.G. ZIMMER, S-integral points on elliptic curves and Fermat's triple equations. In : Algorithmic Number Theory, (J. P. Buhler, ed.), Lecture Notes in Comput. Sci. 1423 (1998), 528-540.

[13] J. H. Silverman, The arithmetic of elliptic curves (Vol. 106). Springer Science and Business Media (2009).

[14] L. C. Washington, (2008). Elliptic curves : number theory and cryptography. CRC press.

[15] D. ZAGIER, Elliptische Kurven : Fortschritte und Anwendungen. Jahresber. Deutsch. Math.- Verein 92 (1990), 58-76.

Résumé :

Dans ce mémoire , nous avons traité deux types d'équations Diophantiennes à savoir les courbes elliptiques et certains ensembles dénommés les m-uplets Diophantiennes. Il s'agit de chercher des ensembles à m entiers (ou rationnels) positifs $\{a_1, a_2, ..., a_m\}$, vérifiant la condition pour $1 \leq a_i < a_j \leq$ m : $a_i a_j + 1$ est un carré parfait. Dans certains cas, nous ramenous ce probléme à la recherche de certains points dans des courbes elliptiques induites pas ces ensembles.

Mots clés: Diophantiennes, courbes elliptiques, m-uplets Diophantiennes.

Abstract :

In this dissertation, we have treated two types of Diophantine equations, namely elliptic curves and certain sets called Diophantine m-tuples. The aim is to find sets with m positive integers (or rationals) $\{a_1, a_2, \dots, a_m\}$, verifying the condition for

$1 \leq a_i < a_j \leq$ m : $a_i a_j + 1$ is a perfect rational square. In some cases, we reduce this problem to the search for certain points in elliptic curves induced by these sets.

Keywords: Diophantine, elliptic curves, called Diophantine m-tuples.

ملخص:

في هذه الأطروحة، عالجنا نوعين من معادلات ديوفانتين، وهما المنحنيات الإهليلجية و مجموعات معينة تسمى ديوفانتين إم – مجموعات. يتضمن هذا البحث عن مجوعات تحوي m من الأعداد الصحيحة الموجبة (أو الناطقة) $\{a_1, a_2, \dots, a_m\}$، تحقق الشرط $a_i a_j + 1$ هو مربع كامل من أجل $1 \leq a_i < a_j \leq$ m. في بعض الحالات، نقوم بتحويل هذه المشكلة إلى البحث عن نقاط معينة في المنحنيات الإهليلجية التي توافق هاته المجموعات.

كلمات مفتاحية: ديوفانتين، المنحنيات الإهليلجية، ديوفانتين إم – مجموعات.