REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique

UNIVERSITE ECHAHID HAMMA LAKHDAR

D'EL OUED

FACULTE DES SCIENCES EXACTES

Mémoire de fin détude

MASTER ACADEMIQUE

Domaine :Mathématiques et informatique

Filiére : Mathématiques

Spécialité : Mathématiques fondamentales

Thème

Équations Diophantiennes liées aux Courbes Elliptiques

Présenté par :

MEKKI Maroua

MEKKI Safa

Sous la Supervision de :

YOUMBAI A. E. Amine

Soutenu devant le jury composé de

S. Ameur Meziane	MCB	Président	Univ. El Oued
A.E.A Youmbai	MAA	Rapporteur	Univ. El Oued
H. Zelaci	MCB	Examinateur	Univ. El Oued

Promotion : 2020/2021

Dédicace

Ce travail est dédié à nos parents.

Remerciement

Mekki safa

Je tiens à remercier toutes les personnes qui ont contribué à m'ont aidé à rédiger ce mémoire.
Tout d'abord, je tiens à remercier mon encadreur.Mr Youmbai Ahmed El Amine, pour sa patience, sa disponibilité et surtout judicieux, qui ont contribué à ma réflexion.
Je remercie également toute l'équipe pédagogique de l'Université Hamma Lakhdar-ElOued
Mes parents, et mon marie pour leur soutien constant et leurs encouragements.

Remerciement

Mekki Maroua

Je tiens à exprimer ma gratitude à mon encadreur,Mr Youmbai Ahmed El Amine.Je le remercie pour ses conseils, sa direction, son aide .
Mes sincères remerciements vont à tous les professeurs, conférenciers, et toutes les personnes qui ont orienté leurs réflexions de leurs paroles, écrits, conseils et critiques et ont accepté de me rencontrer et de répondre à mes questions au cours de mes recherches.
Je remercie mes chers parents, qui ont toujours été là pour moi.
À tous ces conférenciers, j'offre mes remerciements, mon respect et ma gratitude.

Table des matières

Notations **v**

Introduction **1**

1 Courbes elliptiques **3**
1.1 Loi de groupe sur une courbe elliptique 3

2 Taxicab et somme de deux cubes **8**

3 Nombres congruents **15**
3.1 Qu'est-ce qu'un nombre congruent ? 15
3.2 Un moyen de lister les nombres congruents 17
3.3 Un entier qui n'est pas congruent 19
3.4 Rapport avec les courbes elliptiques 20
3.4.1 calcul numérique : 21

4 Solutions rationnelles des équations diophantiennes $f^2(x)+f^2(y)+f^2(z) = n^2$ **23**

Conclusion générale et perspective **28**

Bibliographie **29**

Notations

•A^n Espace affine.
•P^n Espace projectif .
•$\mathbb{T}$: sous groupe de tortion (ensemble des éléments d'ordre fini).
•$\mathbb{K}$ corps.
•$E(\mathbb{K})$ courbe elliptique définie sur le corps $\mathbb{K}$.
• taxicub(n) : le plus petit entier positif qui s'écrit comme somme de deux cubes .
• courbe hyper-elliptique : tout courbe d'équation $y^2 = f(x)$

.

Introduction

Aujourd'hui, les mathématiciens amateurs comme professionnels connaissent les équations diophantiennes et même l'analyse diophantienne. Dans la seconde moitié du 20e siècle, ce domaine des mathématiques est devenu à la mode en raison de sa proximité avec la géométrie algébrique, un foyer apparent de la pensée mathématique. Étonnamment, pratiquement rien n'a été écrit sur diophante, dont le nom est attaché à l'analyse indéterminée et qui est l'un des savants les plus intéressants de l'Antiquité. Même les historiens des mathématiques ont une vision fondamentalement déformée de son travail. La plupart d'entre eux pensent qu'il a résolu des problèmes particuliers, équivalents à des équations indéterminées, au moyen de méthodes particulières et astucieuses.
Dans ce mémoire nous étudions un type particulier des équations Diophantiennes, qui se trouve principalement dans ([3, 6, 10]).
Soit $\{x_1, x_2, ..., x_n\}$ disons X un ensemble de n variables et $f(x_1, x_2, ..., x_n)$ ou tout simplement $f(X)$ un polynôme défini par ces variables à coefficients dans le corps des rationnels. Il n'y aura aucune perte de généralité en supposant que les coefficients sont des nombres entiers (dans $\mathbb{Z}$) puisque nous nous intéresserons aux équations

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

Un n-uple $(x_1^0, x_2^0, ..., x_n^0)$ dans $\mathbb{Z}^n$ satisfaisant $f(x_1^0, x_2^0, ..., x_n^0) = 0$ est appelé solution de l'équation. Une équation ayant une ou plusieurs solutions est dite solvable ou résoluble.
Concernant une équation diophantienne, trois problèmes fondamentaux se posent :
Problème 1. L'équation est-elle résoluble ?
Problème 2. En cas de solvabilité, le nombre de ses solutions est-il fini ou infini ?
Problème 3. En cas de solvabilité, déterminez toutes ses solutions.
Dans ce qui suit, nous traitons 3 problèmes différents, pour les résoudre nous utilisons la théorie des coniques et celle des courbes elliptiques.
Ce mémoire comporte 4 chapitres dont le premier est une généralité sur les courbes elliptiques.
Dans le second, nous présentons un problème dû au mathématicien célèbre S. Ramanujan,

il s'agit de l'écriture de certains entiers comme somme de deux cubes de différent manières. Le troisième chapitre est consacré au plus ancien problème de la théorie des nombres, autrement dit les entiers positifs qui représente l'aire d'un triangle rectangle dont les cotés sont rationnels. Nous avons transformé le problème à la recherche d'un point d'ordre infini sur une courbe elliptique particulière. Nous avons également listé les nombres congruents ≥ 500.
Dans le dernier chapitre nous résolvons (dans $\mathbb{Q}$) une nouvelle équation similaire à ([16, 17]) en utilisant la théorie des courbes elliptiques, le logiciel Magma [1] nous à permis d'effectuer les calculs nécessaires.

Chapitre 1

Courbes elliptiques

La théorie des courbes elliptiques se trouve généralement dans [2, 4, 6, 12, 11]. Nous allons nous intéresser aux courbes définies sur $\mathbb{Q}$ données par l'équation

$$y^2 = x^3 + Ax + B,$$

où A et B sont des rationnels et tel que le discriminant $-(4A^3 + 27B^2)$ du second membre $f(x) = x^3 + Ax + B$ soit différent de zéro. Autrement dit les racines du polynôme f sont distinctes.
Dans le plan projectif $\mathbb{P}^2$ cette équation devient

$$zy^2 = x^3 + Az^2x + Bz^3.$$

Par conséquent la courbe n'a qu'un point à l'infini $O = (0, 1, 0)$ qui est l'intersection de la droite à l'infini d'équation $z = 0$ avec la courbe.

Définition 1.0.1. Une courbe elliptique est une courbe de la forme $E : y^2 = x^3 + Ax + B$ non singulière et irréductible muni d'un point à l'infini.

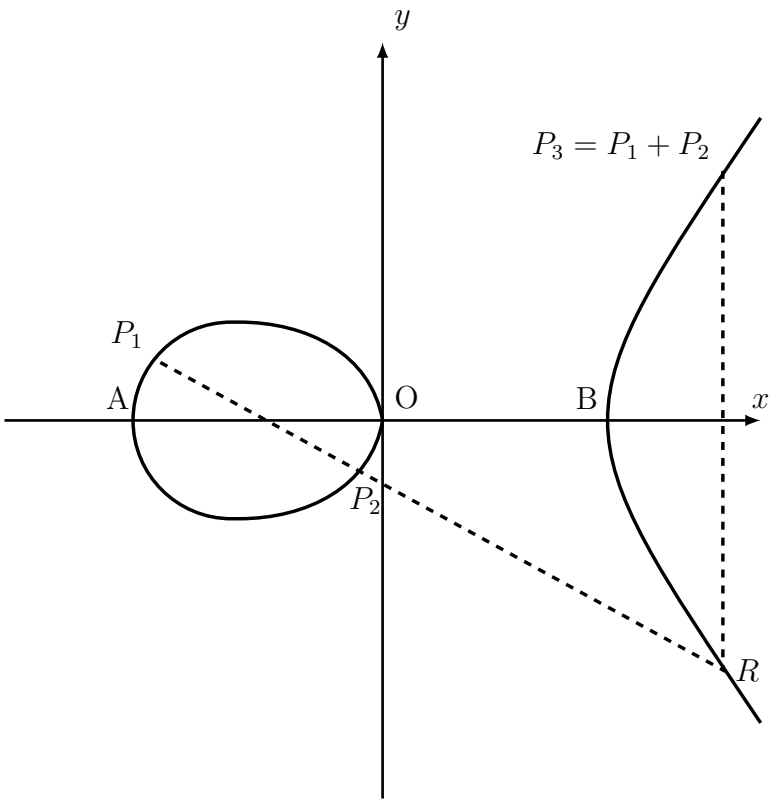
Notation. On note $E(\mathbb{Q})$ l'ensemble des points rationnels de la courbe elliptique E et du point à l'infini O.

1.1 Loi de groupe sur une courbe elliptique

Soit E une courbe elliptique définie sur $\mathbb{Q}$, par l'équation

$$E : y^2 = x^3 + Ax + B. \tag{1.1}$$

Si P_1 et P_2 sont deux points rationnels de la courbe elliptique E et si R est le troisième points d'intersection de la droite P_1P_2 avec la courbe $E(\mathbb{Q})$, on note P_3 le point d'intersection de la courbe avec la droite OR.En posant $P_3 = P_1 + P_2$, on défini sur la courbe $E(\mathbb{Q})$ une structure de groupe abélien d'élément neutre le point à l'infini O.
Le schéma suivant illustre cette opération d'addition :



Si une droite projective intersecte une courbe elliptique (ou tous simplement une cubique) en deux point alors, l'existence d'un troisième point d'intersection est garantie par le théorème suivant.

Théorème 1.1.1 (Bézout)**.** Soit F et G deux courbes algébriques planes de $\mathbb{P}^2(\mathbb{Q})$, de degré m et n, sans composante commune dans $\mathbb{P}^2(\mathbb{Q})$. Alors, F et G se coupent en mn points comptés suivant leurs ordres de multiplicité.

Remarque 1.1.1. L'associativité n'est pas évidente. On peut la démontrer analytiquement mais le calcul est très long. On peut trouver une démonstration purement géométrique dans [Was03] ou une démonstration très courte utilisant la géométrie algébrique (Théorème de Riemann-Roch) dans [4, 12].

On va s'intéresser tout d'abord au sous-groupe des points d'ordre fini de $E(\mathbb{Q})$. On dit un point P de la courbe elliptique E est d'ordre fini s'il existe un entier positif non nul n

tel que :

$$nP = \underbrace{P + P + ... + P}_{n\ fois} = O.$$

Dans ce cas le point P est d'ordre n.

Théorème 1.1.2 (Lutz-Nagell,[18])**.** Soit E une courbe elliptique d'équation

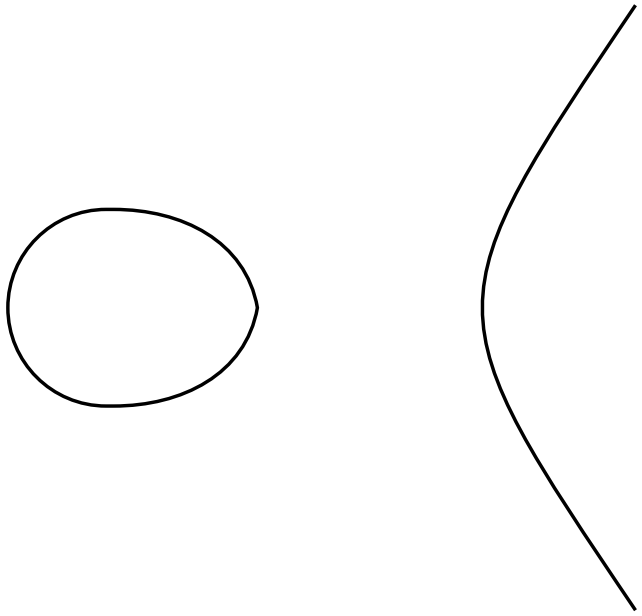
$$E : y^2 = x^3 + Ax + B,$$

où A et B sont dans l'anneau $\mathbb{Z}$, soit $P = (x, y)$ un point de $E(\mathbb{Q})$. Si P est d'ordre fini, alors :

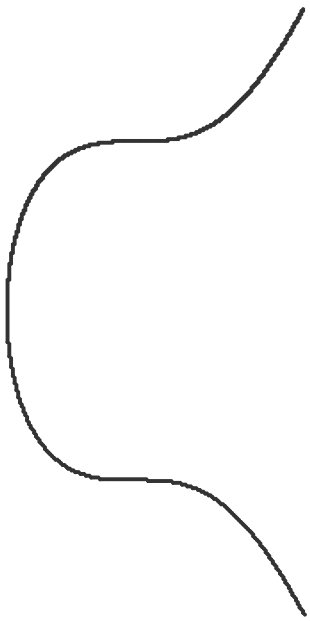
1. x et y sont dans $\mathbb{Z}$.
2. Si $y \neq 0$, alors $y^2 \mid (4A^3 + 27B^2)$.

Géométriquement une courbe elliptique peut prendre deux forme :

Courbe avec deux composantes connexes



Courbe avec une composante connexe



Proposition 1.1.1. *Le sous groupe de torsion de $E(\mathbb{Q})$ est fini.*

Preuve. On se ramène au cas du théorème en faisant comme suit : si $A = \frac{a}{b} \in \mathbb{Q}$ et $B = \frac{c}{d} \in \mathbb{Q}$ avec $a, b, c, d \in \mathbb{Z}^*$ alors on a :

$$bdy^2 = bdx^3 + adx + cb$$

ce qui entraîne

$$b^6d^6y^2 = b^6d^6x^3 + ab^5d^6x + cb^6d^5$$

Et on se ramène au cas du théorème en faisant les changements de variables $Y = b^3d^3y$ et $X = b^2d^2x$. le théorème montre qu'il n'y a qu'un nombre fini de points d'ordre fini. □

Théorème 1.1.3 (Mordell)**.** Le groupe abélien $E(\mathbb{Q})$ est de type fini

$$E(\mathbb{Q}) \simeq \mathbb{T} \oplus L,$$

où $\mathbb{T}$ est un sous groupe fini (les éléments de torsion) et L une partie libre isomorphe à $\mathbb{Z}^r$ ($\mathbb{Z}$-module libre de rang r).

Ce théorème affirme qu'à partir d'un nombre fini de points $\mathbb{Q}$-rationnels d'une courbe elliptique $E(\mathbb{Q})$ on peut générer tout les points de la courbe.

Définition 1.1.1. l'entier non négatif r est le rang de la courbe elliptique E.

Théorème 1.1.4 (Mazur)**.** Soit E une courbe elliptique définie sur $\mathbb{Q}$. Le sous groupe de torsion de $E(\mathbb{Q})$ est isomorphe à l'un des 15 groupes suivants :

$$\mathbb{T} = \begin{cases} \frac{\mathbb{Z}}{n\mathbb{Z}} & 1 \leq n \leq 10 \text{ ou } n = 12, \\ \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{(2n)\mathbb{Z}} & 1 \leq n \leq 4, \end{cases} \tag{1.2}$$

Proposition 1.1.2. *$E(\mathbb{Q})$ est infini si et seulement si le rang r est strictement positif.*

Dans les sections suivantes, nous utilisons les résultats précédents pour résoudre et déterminer les solutions de certaines équations diophantiennes. Les calculs seront faites par le logiciel Magma.

Chapitre 2

Taxicab et somme de deux cubes

Le titre de cette section peut susciter une certaine curiosité puisque nous faisons référence aux modes de transport. La référence à voir avec une célèbre histoire mathématique. Tout au long de l'histoire , les mathématiques ont été criblées de concepts dépassant les fondements d'humbles débuts. Dans cet esprit, de nombreux mathématiciens voient la collaboration, petit et grand, comme une clé importante pour faire progresser leurs domaines respectifs.

Cela se voit facilement au début de XX^e siècle. En 1914, le prodigieux mathématicien, Srinivasa Ramanujan, a quitté sa maison natale de madras en Inde, et s'est rendu à l'université de Cambridge en Angleterre à l'invitation de deux mathématiciens légendaires, G.H Hardy et JE . Littlewood. Un an avant sont arrivée, Ramanujan a envoyé une lettre à Hardy contenant un collage de notation mathématique dispersé dans le texte, à première vue, Hardy a rejeté la lettre et jugé comme du charabia.

Cependant, après un examen plus attentif de Hardy et Littlewood, ils sont arrivés à la conclusion que c'était l'œuvre d'un génie. Cela a commencé une collaboration continue qui a abouti à certains des travaux les plus élégantes jamais produits dans l'histoire des mathématiques.

A la lumière de cela on pourrait dire que le séjour de Ramanujan en Angleterre a été douxamer. Alors qu'il vivait à Cambridge, il est tombé malade en raison des climats contrastés entre l'Angleterre et l'Inde, Hardy a raconté plus tard une histoire sur la visite de Ramanujan pendant sa maladie :

" *Je me souviens être allé le voir une fois alors qu'il était malade à Putney. J'étais monté dans le taxi numéro 1729 et J'avais remarqué que le numéro me paraissent plutôt ennuyeux et que j'espérais que ce n'était pas un présage défavorable. Ramanujan a immédiatement répondu que, au contraire, 1729 est un nombre très intéressant. C'est le plus petit nombre exprimable comme somme de deux cubes de deux manières différentes*".

Ainsi, $1729 = 1^3 + 12^3$ et $1729 = 9^3 + 10^3$ en l'honneur de la conversation Ramanujan Hardy le plus petit nombre exprimable comme la somme de deux cubes de n manières différentes est connu sous le nom du n^{ime} numéro de taxi et est désigné par $taxicab(n)$ par conséquent, avec cette notation, nous voyons que $taxicab(2) = 1729$.
En étendant un peu plus ce concept, un numéro de taxi généralisé peut être défini comme le plus petit nombre pouvant être exprimé comme une somme d'un nombre j de $kième$ puissances dans n différentes manières et est désigné par taxicab(k, j, n) par exemple

$$taxicab(4, 2, 2) = 635318657$$

puisque $635318657 = 59^4 + 158^4$, $635318657 = 133^4 + 134^4$ et le plus petit de ces nombres qui répond aux paramètres donnés par $k = 4, j = 2, n = 2$.
Il est intéressant que personne ne sait quel est le numéro taxicab$(5, 2, n)$ et cela pour tout $n > 1$. Même pour la version faible, aucune solution n'a été fournie. En d'autres termes, si l'on supprime la condition selon laquelle le nombre doit être le plus petit et que l'on laisse $n = 2$, la question peut être reformulée de la manière suivante : Existe-t-il un nombre qui s'exprime comme la somme de deux cinquièmes puissances positives de deux manières différentes ?
Jusqu'à présent, toutes les tentatives pour prouver la version la plus faible ont échoué, une attaque possible est de produire un exemple de manière informatique. Une autre méthode serait de prouver ou de réfuter rigoureusement son existence. Dans tous les cas, ne sous-estimez pas l'efficacité d'une bonne collaboration issue de conversations informelles.
Le numéro de taxi 1729 donne une courbe cubique

$$x^3 + y^3 = 1729$$

qui a deux points entiers, bien sur, nous pouvons changer x et y, donc on se retrouve avec quatre points (9,10), (10, 9) (1, 12) (12, 1) nous prétendons qu'il n'y a pas d'autre points entiers, c'est un cas particulier du théorème de Siegle qui affirme que si C est une cubique non singulière donnée par une équation $f(x, y) = 0$ à coefficients entiers, alors C n'a qu'un nombre fini de points avec des coordonnées entières, pour la démonstration de ce théorème voir ([7, 8]), mais dans ce cas la preuve est facile car le cube $x^3 + y^3$ se décompose en deux facteurs. Alors supposons que x et y sont des entiers satisfaisant $x^3 + y^3 = 1729$ ensuite $(x+y)(x^2-xy+y^2) = 1729 = 7 \times 13 \times 19$ il suffit donc de considérer toutes les factorisations possibles $1729 = AB$ et résoudre les équations simultanées

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

Remplacement $y = (A - x)$ dans la deuxième équation, nous trouvons que

$$3x^2 - 3Ax + A^2 - B = 0.$$

Donc pour chaque factorisation $1729 = AB$, nous devons vérifier si

$$\frac{3A \pm \sqrt{12B - 3A^2}}{6}$$

est un entier.
En effet, nous constatons que nous obtenons des solutions entières uniquement pour les paires $(A, B) = (13, 133)$ et $(A, B) = (91, 19)$ ceus-ci conduit aux quatre solutions connues pour $x^3 + y^3 = 1729$.
Il y a beaucoup d'autres exemples, l'un auquel nous pouvons appliquer ceci et l'autre qui ne peut pas être appliqué, à titre d'exemple :

1. $20683 = 10^3 + 27^3 = 19^3 + 24^3$ alors il y a quatre points (10, 27)(27, 10) (19, 24) (24, 19)
   Donc tous les factorisations possibles de 20683 sont (481, 43) (559, 37) (1591, 13)
   On peut écrire :
   $$20683 = 13 \times 37 \times 43$$
2. 60 c'est un nombre qui ne s'écrit pas comme la somme de deux cubes.

Plus généralement, la plupart des équations cubiques qui prennent en compte la factorisation

$$(ax + by + c)(dx^2 + exy + fy^2 + gx + hy + i) = j$$

avec $j \neq 0$, n'ont qu'un nombre fini de solutions. regardez simplement toutes les factorisations possible $j = AB$ résoudre la paire d'équations $ax + by + c = A$, $dx^2 + exy + fy^2 + gx + hy + i = B$ et voir quelles solutions entières se présentent. Cela pourrait être appelé le cas trivial du théorème de Siegle puisqu'il peut être résolu par un argument élémentaire. Mais il y a encore de nombreuses questions intéressantes que nous pouvons poser sur l'équation de taxi $x^3 + y^3 = m$, et autres équations cubiques pour les quelles le théorème Siegle est trivial, par exemple, nous savons qu'il existe une infinité de solutions mais pouvons nous limiter leur taille ? Bien oui, on peut faire ça plutôt facilement. Nous savons que les solutions satisfont $x + y = A$ et $x^2 - xy + y^2 = B$.
Mais il faut être un peu prudent, depuis une équation stupide comme $x^3 = 1$ a une infinité de solutions parce que y est arbitraire. De même, l'équation $x(x^2 + xy - y) = 1$ a infiniment de nombreuses solutions $(1, y)$

Pour une certaine factorisation $m = AB$. D'où

$$m \geq \mid B \mid = \mid x^2 - xy + y^2 \mid = \frac{3}{4}x^2 + (\frac{1}{2}x - y)^2 \geq \frac{3}{4}x^2$$

D'où $\mid x \mid \leq 2\sqrt{m/3}$, et la même argument donne la même borne pour $\mid y \mid$.
Cela prouve le résultat suivant pour l'équation de "taxicab".

Proposition 2.0.1. Soit $m \geq 1$ un entier, alors chaque solution de l'équation

$$x^3 + y^3 = m$$

en nombres entiers $x, y \in \mathbb{Z}$ satisfait

$$\max\{\mid x \mid, \mid y \mid\} \leq 2\sqrt{m/3}$$

Une autre question naturelle est celle du nombre de solutions. L'observation de Ramanujan est que pour chaque $1 \leq m \leq 1728$, l'équation $x^3 + y^3 = m$ possède au plus une solution en nombres entiers positifs, où nous traitons (x, y) et (y, x) comme la même solution, mais pour $m = 1729$, il existe deux solutions.
Alors nous pourrions demander s'il y a une valeur de m pour lequel il existe trois solutions et quatre solution, etc. La réponse est que pour tout $N \geq 1$ on peut trouver un m telle que l'équation $x^3 + y^3 = m$ possède au moins N solutions.
Pour le prouver, on observe d'abord qu'il y a des équations

$$x^3 + y^3 = m$$

qui ont une infinité de solutions rationnelles. par exemple, considérez la courbe

$$x^3 + y^3 = 9$$

qui a la solution (2,1), il y a essentiellement une correspondance biunivoque entre les points rationnels sur $x^3 + y^3 = 9$ et les points rationnels sur la courbe $y^2 = x^3 - 48$ donné par les formules $X = \frac{12}{x+y}$, $y = 12\frac{x-y}{x+y}$.
Le point $(1, 2)$ sur la courbe $x^3 + y^3 = 9$ correspond au point $Q = (4, 4)$ sur la courbe $Y^2 = X^3 - 48$ Nous calculons $2Q = (28, -148)$ et $3Q = (\frac{73}{9}, \frac{595}{27})$, Ce qui prouve que Q a un ordre infini, parce que le théorème de Lutz-Nagel dit que les points d'ordre fini ont des coordonnées entieres . D'où les deux équations $Y^2 = X^3 - 48$ et $x^3 + y^3 = 9$ ont une infinité de points rationnels.

Puisqu'il y a une infinité de points rationnels sur $x^3 + y^3 = 9$, nous pouvons trouver certainement N points distincts, dit $P_1, ..., P_N$ si $p = (\frac{a}{b}, \frac{c}{d})$ est un point rationnel écrit en termes les plus bas avec des dénominateur positifs, puis en remplaçant dans l'équation et la compensation des dénominateurs donne

$$a^3d^3 + c^3d^3 = 9b^3d^3.$$

Ainsi b^3 divise a^3d^3 et d^3 divise c^3b^3. Mais $pgcd(a, b) = 1$ et $pgcd(c, d) = 1$, donc b^3/d^3 et d^3/b^3, et par conséquent $b = d$. Cela signifie que nous pouvons écrire les coordonnées de $P_1, ..., P_N$ comme $P_1 = (\frac{a_1}{d_1}, \frac{c_1}{d_1}), ..., P_N = (\frac{a_N}{d_N}, \frac{c_N}{d_N})$. Maintenant pour l'idée principale nous choisissons un m en substituant efface le dénominateurs des P_i, les transformant ainsi en point entiers. Les P_i sont sur la courbe $x^3 + y^3 = 9$, alors nous laissons

$$D = d_1.d_2...d_N$$

et prendre $m = 9D^3$ puis le points $P'_i = (\frac{D_{a_i}}{d_i}, \frac{D_{c_i}}{d_i})$ pour $i = 1, ..., N$ ont des coordonnées entiers et sont sur la courbe

$$x^3 + y^3 = 9D^3.$$

Cela prouve notre affirmation, que nous reformulons comme une proposition formelle.

Proposition 2.0.1. *Pour chaque entier $N \geq 1$ il y a un entier $m \geq 1$ tel que la courbe cubique $x^3 + y^3 = m$ a au moins N points avec des coordonnées entiers.*

Bien sur, cela ne généralise par strictement l'exemple de Ramanujan, car il ne concernait que les sommes de cubes positifs. Cependant, il n'est pas difficile de prouver que si $m > 0$ et si la courbe $x^3 + y^3 = m$ a une infinité des solutions rationnelles, alors il existe une infinité des solutions rationnelles avec x et y tous les deux positifs. L'idée est que l'ensemble des points réels sur cette courbe ressemble au groupe de cercles, donc le sous-groupe généré par un point d'ordre infini est dense dans l'ensemble de points réels. Puisqu'il y a de vrais points avec $x, y > 0$
Cela montre que si nous prenons m assez large puis l'équation $x^3 + y^3 = m$, peut avoir un nombre arbitrairement grand de solutions entières positives . Mais l'observation de Ramanujan était également que 1729 est le plus petit m avec deux solutions positives.
Alors quel est le plus petit m qui a trois solutions positives ?
La réponse se trouve dans [11]
$87539319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3$.

Taxicab et somme de deux cubes

Basé sur l'histoire de Hardy-Ramanujan, les gens ont défini le numéro N Taxi à être

$$Taxi(N) = min\{m \geq 1 : x^3 + y^3 = m\}$$

. a au moins N entier solution avec $x \geq y > 0$
Alors $Tax(2) = 1729, Taxi(3) = 87539319$
La preuve que nous avons donnée de la Prop 2.0.1 peut être transformé en (trés pauvre) borne superieure pour $Taxi(N)$, mais en pratique, il est assez difficile de déterminer exactement $Taxi(N)$ en raison du difficulté à exclure les m plus petits qui pourraient fonctionner.
Voici l'état actuel (à partir de 2015) :
$Taxi(1) = 2$
$Taxi(2) = 1729$
$Taxi(3) = 87539319$
$Taxi(4) = 6963472309248$
$Taxi(5) = 48988659276962496$
$Taxi(6) = 24153319581254312065344$
Sans surprise, les numéros de taxi ont de nombreux facteurs.
Par exemple,

$$Taxi(6) = 2^6.3^3.7^4.13.19.43.73.79^3.97.157$$

En quelque sortes, Prop 2.0.1 fournit une réponse satisfaisante à notre question sur le nombre de points entiers qu'une courbe cubique peut avoir. Mais ça peut partir vous êtres un peu inquiet car nous n'avons pas vraiment trouvé beaucoup de points intrinsèquement intégraux. Au lieu, nous avons trouvé beaucoup de points rationnels et effacé sur dénominateurs.
Cela conduit à des solutions (x, y) dans lequel x et y ont tendance à avoir un grand facteur commun. Si nous refusons les facteurs communs, nous sommes conduits au question suivante.
Étant donné un entier N, est-il possible de trouver un entier $m \geqslant 1$ de sorte que l'équation $x^3 + y^3 = m$ a au moins N entier solution avec $x \geq y > 0$ et $pgcd(x, y) = 1$ pour $N = 2$ la réponse est oui, puisque $1729 = 12^3 + 1^3 = 10^3 + 9^3$. Pour $N = 3$, la réponse est aussi oui, découverte par Paul Vojta en 1983 via un calcul de 3 jour sur un ancien ordinateur de bureau. Le numéro de Vojta est 15170835645

$$= 2468^3 + 517^3$$

$$= 2456^3 + 709^3$$

$$= 2152^3 + 1733^3$$

. Deux décennies plus tard, Stuart Gascoigne et Duncan Moore (indépendamment) ont trouvé un exemple avec quatre représentation du nombre 1801049058342701083

$$\begin{aligned} &= 1216500^3 + 92227^3 \\ &= 1216102^3 + 1366635^3 \\ &= 1207602^3 + 341995^3 \\ &= 1165884^3 + 600259^3. \end{aligned}$$

Et c'est là que se situe la situation.Personne ne sait si la réponse pour $N = 5$. Nous concluons cette section en discutant d'une relation intéressante entre le nombre de points rationnels. Serge Lang fait une conjecture générale qui a été prouvée pour certains types de courbes cubiques, y compris les courbes de taxis étudiées dans cette section

Théorème 2.0.1. (Silverman [10]) Il y a une constante $K > 1$ avec la propriété suivante. Pour chaque entier $m \geq 1$, le nombre points d'entiers relativement premiers sur la courbe cubique

$$C_m : x^3 + y^3 = m$$

est borné par le rang du groupe de points rationnels via l'estimation

$$\{(x, y) \in C_m(\mathbb{Q}) : x, y \in \mathbb{Z} \text{ et } pgcd(x, y) = 1\} \leq K^{1+rankC_m(\mathbb{Q})}.$$

Le Théorème (2.0.1) dit que les points entiers avec $pgcd(x, y) = 1$ ont tendance à être quelque peu linéairement indépendants dans le groupe des points rationnels.
En particulier, si on pourrait trouver une séquence de m de sorte que le nombre de ces points entiers va à l'infini alors on pourrait conclure que les rangs vont à l'infini. Inversement, si l'on pouvait prouver que le rang de $C_m(\mathbb{Q})$ est borné indépendant de m, ensuite il en serait de même pour le nombre de points entiers sans facteur commun.

Chapitre 3

Nombres congruents

3.1 Qu'est-ce qu'un nombre congruent ?

La question discutée dans cet section est très simple à poser. Un peu à l'instar du théorème de Fermat [1], cet énoncé fort simple d'arithmétique cache énormément de mathématiques compliquées que nous allons donc essayer de présenter.

Un entier n est dit congruent s'il est l'aire d'un triangle rectangle à côtés rationnels. Autrement dit n est congruent si et seulement s'il existe trois rationnels non nuls a, b et c tels que :

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2n. \end{cases}$$

Il s'agit d'une question très ancienne, qui aurait pu par exemple être posée par Diophante [2]. bien que cela n'ait pas été le cas. Au sens strict, elle n'est pas encore résolue aujourd'hui ; toutefois, on a une idée conjecturale d'une solution très acceptable.

Mais examinons plutôt l'énoncé donné ci-dessus. On peut se demander pourquoi n est supposé être entier alors que les côtés a, b et c sont simplement supposés rationnels. En fait, cela n'a pas grande importance car il est équivalent de chercher les n entiers et les n rationnels. Plus précisément si le rationnel $\frac{u}{v}$ est congruent alors il en est de même de l'entier

1. Le théorème dit qu'il n'existe pas d'entiers strictement positifs x, y et z vérifiant $x^n + y^n = z^n$ lorsque n est un entier supérieur ou égal à 3.

2. Diophante a posé nombre de questions similaires ; il a d'ailleurs laissé son nom aux équations diophantiennes qui est un terme générique pour désigner les équations dont on ne cherche que les solutions entières (ou rationnelles)

uv et réciproquement. En effet si l'on peut trouver a, b et c tels que :

$$\begin{cases} a^2 + b^2 = c^2 \\ ab = 2\frac{u}{v}. \end{cases}$$

alors on peut écrire directement :

$$\begin{cases} (av)^2 + (bv)^2 = (cv)^2 \\ (av)(bv) = 2uv. \end{cases}$$

La réciproque est tout aussi immédiate.

Plus généralement, si r et s sont deux rationnels, le rationnel r est congruent si et seulement si le rationnel rs^2, l'est. Autrement dit, pour la propriété de congruence, on peut regarder les rationnels à multiplication par un carré près. Or si on se donne un rationnel, en le multipliant par un carré on peut le faire devenir entier, mais on peut aussi, en choisissant bien le carré, faire en sorte que les exposants qui interviennent dans la décomposition en facteurs premiers de cet entier ne soient jamais supérieurs ou égaux à 2. Un tel entier est dit sans facteur carré, et en effet le seul carré qui le divise est 1.

Bref, on peut se contenter pour la question originale de regarder les entiers n qui sont sans facteur carré. Ce ne sera pas franchement intéressant par la suite, mais c'est quand même une remarque à avoir en tête.

En fait, trouver des nombres congruents est chose simple. On commence par déterminer ce que l'on appelle un triplet Pythagoricien, c'est-à-dire trois entiers a, b et c tels que $a^2+b^2 = c^2$ et on calcule bêtement le produit $\frac{ab}{2}$ qui donne donc un entier congruent.

Évidemment, il reste à déterminer des triplets Pythagoriciens ce qui n'est pas forcément facile pour celui qui ne connaît pas. Mais pour commencer, on peut y aller au petit pas et tomber par exemple sur le triplet (3, 4, 5) si on ne le connait pas déjà. Ainsi on trouve que $\frac{3\times4}{2} = 6$ est un entier congruent. On peut ensuite trouver le triplet (5, 12, 13) ce qui donne l'entier congruent 30.

Enfin, on peut donner la formule suivante :

$$(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$$

formule qui permet d'obtenir toute une famille de triplets pythagoriciens et donc de nombres congruents.

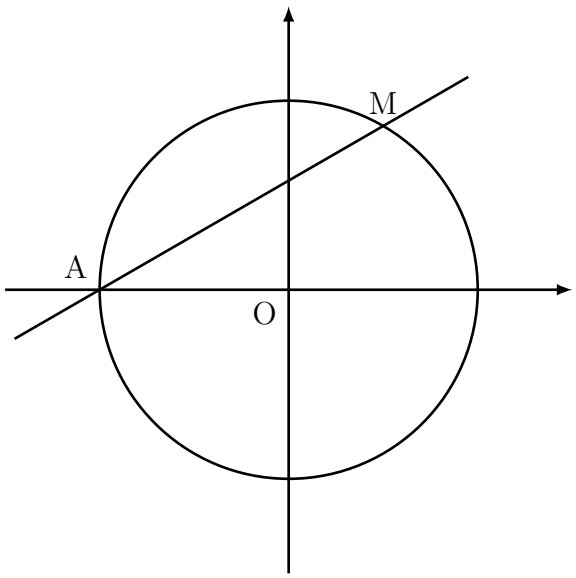
3.2 Un moyen de lister les nombres congruents

Précédemment, nous avons donné une formule pour obtenir toute une famille de nombres congruents. Nous allons voir ici qu'en fait, ce sont les seuls. Plus exactement, on a le théorème suivant :

Théorème 3.2.1. Si a et b sont deux rationnels tels que $a^2 + b^2 = 1$ et $a \neq -1$, alors il existe un rationnel t tel que

$$a = \frac{1 - t^2}{1 + t^2} \quad et \quad b = \frac{2t}{1 + t^2}.$$

Ce théorème est en fait très facile à démontrer lorsque l'on a la bonne idée. L'ensemble des points du plan de coordonnées (x, y) vérifiant la relation $x^2 + y^2 = 1$ est le cercle de centre l'origine est de rayon 1.



On place sur la figure le point A de coordonnées $(-1, 0)$ et le point M de coordonnées (a, b). Ce sont tous deux des points du cercle à coordonnées rationnelles. Ainsi la pente de la droite (AM) est un nombre rationnel, disons t. Finalement l'équation de cette droite est $y = t(x + 1)$.
Pour trouver a et b, il ne reste plus qu'à déterminer l'intersection de cette droite avec le cercle. On est donc amené à résoudre le système :

$$\begin{cases} x^2 + y^2 = 1 \\ y = t(x + 1), \end{cases}$$

On obtient ainsi $x^2+t^2(x+1)^2=1$. Bien sûr $x=-1$ est solution de cette équation de degré 2. Comme la somme des deux racines doit faire $\frac{2t^2}{1+t^2}$, on en déduit que :

$$a=\frac{-2t^2}{1+t^2}+1=\frac{1-t^2}{1+t^2}$$

On trouve ensuite facilement la valeur de b.
On constate plusieurs choses. Premièrement, si l'on ne cherchait que les a et b strictement positifs, il suffirait de se limiter aux rationnels t compris strictement entre 0 et 1, comme on le voit directement sur la figure.
Ensuite, ce théorème permet de déterminer complètement les triplets pythagoriciens :

En effet, si (a,b,c) est un tel triplet, on a $\left(\frac{a}{c}\right)^2+\left(\frac{b}{c}\right)^2=1$ et on est alors ramené au problème précédent. En écrivant ensuite $t=\frac{m}{n}$, on voit que les solutions données précédemment sont les seules, à permutation près de a et b, et à multiplication par un même entier près.
Enfin, cette classification permet de donner un algorithme pour lister tous les nombres congruents. Si l'on se restreint aux positifs disons[3], on voit qu'il suffit de commencer par lister tous les rationnels compris entre 0 et 1 et pour chacun d'eux de calculer l'expression $\frac{t(1-t^2)}{(1+t^2)^2}$ ou plus simplement l'expression $t(1-t^2)$,et éventuellement ensuite renormaliser le nombre en le multipliant par le bon carré pour qu'il devienne un entier sans facteur carré.
Il n'est alors pas difficile, avec ce que l'on a fait précédemment, de se convaincre que l'on n'aura ainsi oublié aucun nombre.
Lister les nombres rationnels compris entre 0 et 1 n'est pas difficile. On commence par mettre ceux dont le dénominateur est 2, c'est-à-dire simplement $\frac{1}{2}$. Viennent ensuite ceux dont le dénominateur est 3, donc $\frac{1}{3}$ et $\frac{2}{3}$. Puis on passe à 4 (bien sûr, ce n'est pas la peine de mettre $\frac{2}{4}$ qui y est déjà). On obtient donc une liste qui commence ainsi :

$$\frac{1}{2},\frac{1}{3},\frac{2}{3},\frac{1}{4},\frac{3}{4},\frac{1}{5},\frac{2}{5},\frac{3}{5},\frac{4}{5},\frac{1}{6},\frac{5}{6},\frac{1}{7},\frac{2}{7},\frac{3}{7},\cdots$$

En faisant donc le calcul annoncé pour chaque rationnel listé précédemment, on obtient le début de la liste des nombres congruents :

$$6,6,30,15,21,30,210,15,5,210,330,21,70,210,...$$

3. Ce qui n'est pas absurbe, vu qu'à l'origine un tel nombre représente l'aire d'un triangle rectangle.

On remarque que de nombreux entiers peuvent être listés plusieurs fois, mais en tout cas, une chose est sûre c'est qu'on les obtient ainsi tous.
Seulement la question que l'on aimerait résoudre, c'est savoir, étant donné un entier n, s'il est congruent ou non. S'il est congruent, bien sûr, on peut s'en sortir : on fait la liste et on attend qu'il tombe. Mais s'il ne l'est pas, on ne pourra jamais le savoir par ce moyen. En outre, ce n'est pas dit qu'un entier congruent arrive rapidement dans la liste précédente. Par exemple l'entier $n = 157$ qui est congruent arrive seulement pour :

$$t = \frac{(526771095761)^2}{(157841)^2 \times (4947203)^2}$$

ce qui correspond quand même à un rationnel relativement complexe, loin dans la liste.

3.3 Un entier qui n'est pas congruent

Si l'on a trouvé des entiers congruents, on ne sait toujours pas à ce stade s'il en existe qui ne le sont pas. Et pourtant il ne faut pas chercher loin : ni l'entier 1, ni l'entier 2 ne sont congruents par exemple.
Le premier exemple démontré est celui de l'entier 1 et la démonstration remonte à Fermat.

Il s'agit donc de prouver qu'il n'existe pas d'entiers non nuls a, b, c et d vérifiant le système d'équations suivant :

$$\begin{cases} a^2 + b^2 = c^2, \\ ab = 2d^2. \end{cases}$$

Supposons qu'une telle solution existe et voyons ce que cela implique. Déjà, dans un premier temps, on peut supposer que a et b sont premiers entre eux. Si ce n'était pas le cas, leur Pgcd diviserait à la fois c et d et on pourrait diviser les quatre entiers par ce Pgcd, obtenant ainsi à une autre solution pour laquelle a et b sont premiers entre eux.
D'après ce que l'on a alors plus ou moins vu précédemment, on sait qu'il existe des entiers encore premiers entre eux m et n tels que par exemple :

$$a = m^2 - n^2; \quad b = 2mn; \quad c = m^2 + n^2$$

Le produit ab vaut alors d'une part $2d^2$ et d'autre part $2mn(m^2 - n^2)$. Les entiers m et m^2-n^2 sont premiers entre eux car si x était un diviseur commun de ces nombres, alors il diviserait à la fois m et n^2 et devrait donc forcément valoir 1. De même, n et m^2-n^2 sont premiers entre eux. Ainsi, $mn(m^2 - n^2)$ est le produit de trois nombres premiers entre eux

et c'est un carré. Chacun des facteurs est donc un carré. Autrement dit, il existe des entiers $p,\ q\ et\ r$ tels que :

$$m = p^2 \ \ ; \ \ n = q^2 \ \ ; \ \ m^2 - n^2 = r^2$$

Mais alors $r^2 = p^4 - q^4 = (p^2 - q^2)(p^2 + q^2)$. Ces deux facteurs sont encore premiers entre eux, et donc sont tous les deux des carrés.
Ainsi on vient de prouver que si 1 est congruent, alors il existe deux entiers strictement positifs, disons s et t, tels que les quatre nombres $s,\ t,\ s+t\ et\ s-t$ soient tous des carrés. Et nous allons montrer maintenant que ce dernier fait est impossible.
Pour ce faire, on utilise le principe de descente infinie : on suppose que de tels entiers existent, et à partir de ces entiers, on en construit d'autres, encore solutions du problème, et plus petits. Si l'on arrive à faire cela, on aura bien prouvé qu'il n'existe pas de solution. En effet, s'il en existait une, on pourrait construire éternellement une solution toujours plus petite, et ceci entre en contradiction avec le fait qu'il n'existe pas de suite infinie d'entiers strictement décroissante.
Supposons donc que $s = p^2,\ t = q^2,\ s+t = u^2\ et\ s-t = v^2$. Alors $u^2-v^2 = (u+v)(u-v) = 2q^2$. Comme $u\ et\ v$ ont forcément la même parité, les entiers $u+v$ et $u-v$ sont tous les deux pairs, et donc on a par exemple $u-v = 4a^2$ et $u+v = 2b^2$. Mais alors $p^2 = v^2+q^2 = b^4+4a^4$ et on retrouve par le fait un triplet pythagoricien. On écrit donc :

$$b^2 = s'^2 - t'^2 \ \ ; \ \ 2a^2 = 2s't' \ \ ; \ \ p = s'^2 + t'^2$$

où s' et t' sont des entiers premiers entre eux. La seconde égalité prouve que s' et t' sont tous les deux des carrés. La première prouve que $s'+t'$ et $s'-t'$ en sont aussi. À l'évidence la troisième égalité prouve quant à elle que $s' < s$, la solution est donc plus petite en ce sens. Cela conclut.
Avec des méthodes qui ressemblent par certains points, on devrait réussir à démontrer que 2 non plus n'est pas congruent. Cela dit, maintenant, on aimerait une méthode un peu plus systématique pour savoir si un entier donné est ou n'est pas congruent. C'est ce que nous allons exposer par la suite.

3.4 Rapport avec les courbes elliptiques

On a vu que l'entier n était congruent si et seulement s'il est égal, à un carré près, à un nombre de la forme $t(1-t^2)$ pour un certain rationnel t. Une formulation équivalente est

de dire que n est congruent si et seulement s'il existe deux rationnels s *et* t tels que :

$$s^2n = t(1-t^2) = t - t^3$$

Ou encore, en multipliant tout par n^3 :

$$(sn^2)^2 = n^2(tn) - (tn)^3 = (-tn)^3 - n^2.(-tn)$$

Ainsi en posant $x = -tn$ et $y = sn^2$, on obtient $y^2 = x^3 - n^2x$.
Le calcul précédent prouve plus ou moins que l'entier n est congruent si et seulement s'il existe deux rationnels x et y, avec $y \neq 0$, tels que $y^2 = x^3 - n^2x$.

Remarque 3.4.1. L'équation que nous avons obtenu est une courbe elliptique.

Appelons E_n la courbe elliptique correspondant à l'équation $y^2 = x^3 - n^2x$, c'est-à-dire si l'on préfère au couple $[-n^2, 0]$ une notation largement utilisée. Notre but consiste donc à étudier les points rationnels de E_n, c'est-à-dire l'ensemble $E_n(\mathbb{Q})$ Dans un premier temps, plutôt, nous allons dessiner $E_n(\mathbb{R})$ pour avoir une idée. C'est évidemment plus facile car l'on sait facilement reconnaître les carrés dans $\mathbb{R}$: ce sont exactement les nombres positifs ou nuls. On cherche donc juste à savoir pour x fixé si la quantité $x^3 - n^2x$ est positive ; lorsque c'est le cas, il y a deux solution en y, sinon il n'y en a pas.

3.4.1 calcul numérique :

Passons maintenant au calcul avec le logiciel Magma [1] pour déterminer les nombres congruents inférieurs à 25.
> for n := 1 to 25 do
for > E :=EllipticCurve([0,0,0,-n^2,0]) ;
for > Rank(E) ;
for > end for ;
Si le rang est non nul, alors la courbe $y^2 = x^3 - n^2x$ possède un point d'ordre infini ce qui montre que l'entier n est congruent.

Remarque 3.4.2. Sachez qu'il n'existe aucune formule ou algorithme qui garantit le calcul du rang d'une courbe elliptique.

Les résultats sont lister dans le tableau suivant :

TABLE 3.1 – Nombres Congruents

n	$Rank(E_n)$	
1	0	(non congruent)
2	0	(non congruent)
3	0	(non congruent)
4	0	(non congruent)
5	1	(congruent)
6	1	(congruent)
7	1	(congruent)
8	0	(non congruent)
9	0	(non congruent)
10	0	(non congruent)
11	0	(non congruent)
12	0	(non congruent)
13	1	(congruent)
14	1	(congruent)
15	1	(congruent)
16	0	(non congruent)
17	rank computed (0) is only a lower bound	Indéterminé
18	0	(non congruent)
19	0	(non congruent)
20	1	(congruent)
20	1	(congruent)
21	1	(congruent)
22	1	(congruent)
23	1	(congruent)
24	1	(congruent)
25	0	(non congruent)

Chapitre 4

Solutions rationnelles des équations diophantiennes $f^2(x)+f^2(y)+f^2(z)=n^2$

Dans cette section, nous discutons les solutions rationnelles des équations diophantiennes $f^2(x)+f^2(y)+f^2(z)=n^2$. Ce problème peut être résolu par la théorie des courbes elliptiques, Inspiré par le travail de M. Ulas et A. Togbé [15] (Publ Math Debrecen 76(1-2) :183-201, 2010) nous montrons que l'équation en titre, possède une infinité de solutions rationnelles.

Historique du problème

Soit $f(x) \in \mathbb{Q}[x]$ un polynôme sans racines multiples et considérons les équations Diophantiennes

$$z^2 = f^2(x) + f^2(y) \tag{4.1}$$

et

$$z^2 = f^2(x) - f^2(y) \tag{4.2}$$

Le problème remonte à 2010 lorsque Ulas et Togbé ont montré que si $f(x)$ est de degré 2 alors l'ensemble des solutions paramétriques rationnelles des équations

$$f^2(x) \pm f^2(y) = z^2 \tag{4.3}$$

n'est pas vide et si $deg(f) = 3$ et f a la forme $f(x) = x(x^2+ax+b)$ avec $a \neq 0$, alors (4.3) a une infinité de solutions paramétriques rationnelles non triviales. Ils ont également prouvé la même chose pour des polynômes cubiques plus généraux de la forme $f(x) = x^3 + ax^2 + b$ avec $b \neq 0$ pour Éq. (4.2) et se sont demandé s'il existe un polynôme de degré supérieur tel que l'une ou les deux Éqs. (4.1) et (4.2) sont satisfaites pour une infinité de solutions rationnelles non triviales (x, y, z). Nous mentionnons également un article étroitement lié de Tengely et Ulas [14] dans lequel ils ont étudié l'existence de solutions intégrales des équations diophantiennes $z^2 = f(x)^2 \pm g(y)^2$, pour certains polynômes $f,\ g \in \mathbb{Z}[x]$ de degré au moins 3.

En octobre 2018, Zhang et Zargar [17] ont répondu à la question d'Ulas et Togbé en utilisant des polynômes quartiques. Récemment , Youmbai et Behloul dans [16] ont amélioré certains résultats dans [17] en prouvant pour certains polynômes de degré $2n+3$ ($n \in \mathbb{N}$) que les deux éq. (4.1) et (4.2) ont une infinité de solutions rationnelles non triviales paramétrées par certaines courbes elliptiques quartiques de rang positif. Ensuite, à l'aide d'une méthode élémentaire, les auteurs ont généralisé ce résultat et résoudre le problème d'une manière différente en utilisant des polynômes $f(x)$ de toute degré n pour les deux équations. (4.1) et (4.2) en montrant qu'il existe une infinité de solutions non triviales rationnelles paramétrées par des sections coniques. Bref, il ont montré les théorèmes suivants

Théorème 4.0.1. Soit

$$f(x) = x\left(\prod_{t=0}^{n}\left(x-k^t\right)\left(x+k^t\right)\right).$$

Pour $k = \left(\frac{2h}{h^2-1}\right)$ et $h \neq 0, \pm 1$, l'équation diophantienne $f^2(x) + f^2(y) = z^2$ a infiniment de nombreuses solutions rationnelles non triviales.

Théorème 4.0.2. Soit

$$f(x) = x\left(\prod_{i=0}^{n}\left(x-k^t\right)\left(x+k^t\right)\right)$$

Pour $k = \left(\frac{2h}{k^2+1}\right)$ et $h \neq 0, \pm 1$, l'équation diophantienne $f^2(x) - f^2(y) = z^2$ a infiniment de nombreuses solutions rationnelles non triviales.

Théorème 4.0.3. Soit

$$f(x) = x\left(\prod_{t=0}^{n}\left(x+k^t\right)\right)$$

Pour $k = \left(\frac{2h}{k^2-1}\right)$ et $h \neq 0, \pm 1$,l'équation diophantienne $f^2(x) + f^2(y) = z^2$ a infiniment de nombreuses solutions rationnelles non triviales.

Théorème 4.0.4. Soit

$$f(x) = x\left(\prod_{f=0}^{n}\left(x+k^t\right)\right).$$

Pour $k = (\frac{2h}{h^2+1})$ et $h \neq 0, \pm 1$, l'équation diophantienne $f(x)^2 - f(y)^2 = z^2$ a infiniment de nombreuses solutions rationnelles non triviales.

Pour prouver les théorèmes (4.1) et (4.2), il suffit de démontrer le lemme suivant

Lemme 4.0.1. Soit C : $v^2 = au^4 + bu^2 + c^2$. une courbe hyper-elliptique sur $\mathbb{Q}$ tel que

$$a \neq 0, \quad c \neq 0$$

$$a \text{ et } (b^2 - 4ac^2), \text{ ne sont pas des carrs rationnels.}$$

Alors, les déclarations suivantes sont valables.

1. La courbe hyper-elliptique C est bi-rationnellement équivalente à une courbe elliptique avec une équation de Weierstrass

$$E : \ y^2 = x^3 + bx^2 + ac^2x.$$

2. La courbe elliptique associée de C a un sous-groupe de torsion isomorphe à $\frac{\mathbb{Z}}{2\mathbb{Z}}$.

Preuve 4.0.1. 1. En multipliant les deux membres de C par a^2u^2, on obtient

$$(auv)^2 = (au^2)^3 + b(au^2)^2 + ac^2(au^2).$$

Ceci montre que C est bi-rationnellement équivalent à la courbe elliptique E définie ci-dessus. Pour en savoir plus sur la façon de transformer l'équation d'une courbe elliptique du Modèle de Weierstrass au modèle quartique et vis-versa voir ([[6], p. 37] et [18]).

2. On sait que ce modèle de courbe hyper-elliptique a un sous-groupe de torsion $\frac{\mathbb{Z}}{2K\mathbb{Z}}$ ou $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2K\mathbb{Z}}$, pour certains entier pair k. Le point $(x, y) = (0, 0)$ se trouve dans E et puisque $y = 0$, ce point est d'ordre 2. Afin d'éliminer ces groupes de la forme $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2K\mathbb{Z}}$ nous devons prouver que $(0, 0)$ est le seul point d'ordre 2. En effet, le second terme de E factorise comme $x(x^2 + bx + ac^2)$ et $(x^2 + bx + ac^2)$ est irréductible dans $\mathbb{Q}[x]$ puisque $b^2 - 4ac$. (le discriminant de $x^2 + bx + ac^2$) est supposé ne pas être un carré rationnel. Pour finir le preuve nous devons juste nous assurer que E n'a pas de point d'ordre quatre. Si un point $P = (Z, W)$ est dans E alors la coordonnée x de $2P$ est

$$\frac{(Z^2 - (ac^2))^2}{4W^2},$$

De cette façon, si P est d'ordre quatre alors $x(2P) = x(0, 0) = 0$, ce qui signifie $Z^2 = (ac^2)$. mais selon les conditions du Lemme 4.0.1 , a est supposé ne pas être un rationnel carré. Par conséquent, E ne peut pas avoir un point d'ordre quatre et le sous-groupe de torsion de E ne peut être que $\frac{\mathbb{Z}}{2\mathbb{Z}}$.

Dans ce qui suit, nous traitons un problème similaire en utilisant certains polynômes de degré 5. Il s'agit de monter que l'équation suivante :

$$f^2(x) + f^2(y) + f^2(z) = n^2 \tag{4.4}$$

possède une infinité de solutions rationnelles (x, y, z, n). Considérons le polynôme sans racines multiples :

$$f(x) = x\left(\prod_{t=0}^{3}\left(x + k^t\right)\right). \tag{4.5}$$

En utilisant les substitutions $x = T$, $y = kT$ et $z = k^2T$ l'équation 4.4 se réduit à

$$n^2 = \left(T\left(\prod_{t=0}^{n}\left(T + k^t\right)\right)\right)^2 + \left(kT\left(\prod_{t=0}^{n}\left(kT + k^t\right)\right)\right)^2 + \left(k^2T\left(\prod_{t=0}^{n}\left(k^2T + k^t\right)\right)\right)^2.$$

puis après avoir rassemblé les carrés en communs, nous aurons :

$$n^2 = (M)^2\left(AT^4 + BT^3 + CT^2 + DT + E\right).$$

Posons H l'équation

$$s^2 = AT^4 + BT^3 + CT^2 + DT + E.$$

Maintenant pour prouver l'existence d'infinité de solutions rationnelles pour cette équation, il suffit de montrer que H possède une infinité de points. En effet, la courbe hyperelliptique H est équivalente à une courbe elliptique, on peut obtenir son équation via des changement de variables admissibles (voir [18]). Si la courbe possède un rang strictement positif, alors le problème est résolu.

Exemple 4.0.1. Soit $k = 2$, considérons le polynôme

$$f(x) = x\left(\prod_{t=0}^{3}\left(x + 2^t\right)\right).$$

Considérons maintenant l'équation :

$$n^2 = f^2(x) + f^2(y) + f^2(z)$$

En utilisant les substitutions $x = T$, $y = 2T$ et $z = 4T$ l'Eq. 4.4 de réduit à :

$$n^2 = x^2(x+2)^2(x+1)^2[1049601x^4 + 1582104x^3 + 877008x^2 + 215808x + 21504].$$

Posons H la courbe d'équation

$$s^2 = 1049601x^4 + 1582104x^3 + 877008x^2 + 215808x + 21504.$$

La courbe H est équivalente à la courbe elliptique d'équation

$$E : y^2 + xy + y = x^3 - x^2 - 1277537x + 293902449$$

En utilisant le logiciel magma en peut obtenir les informations nécessaire sur E.
> C :=HyperellipticCurve([1049601,1582104,877008,215808 ,21504]) ;
> E :=AssociatedEllipticCurve(C) ;
> SetClassGroupBounds("GRH") ;
> E ;
Elliptic Curve defined by $y^2 + x * y + y = x^3 - x^2 - 1277537x + 293902449$ over Rational Field
> DescentInformation(E) ;
Torsion Subgroup is trivial
The 2-Selmer group has rank 4
Found a point of infinite order.
Found 2 independent points.
Found 3 independent points.
Found 4 independent points.
After 2-descent :
4 <= Rank(E) <= 4
Sha(E)[2] is trivial
(Searched up to height 100 on the 2-coverings.)
$[4, 4]$
$[(3207 : -172404 : 1), (1037 : -9654 : 1), (5723/4 : 292893/8 : 1), (-1231 : 552 : 1)]$

Le résultat indique que H est équivalente à la courbe elliptique $E : y^2 + x * y + y = x^3 - x^2 - 1277537x + 293902449$ qui est de rang 4. Cela implique que H possède une infinité de points rationnels et par conséquence l'équation 4.4 possède également une infinité de solutions rationnelles (x, y, z, n).

Conclusion générale et perspectives

Nous sommes arrivés au terme de ce mémoire, que nous avons préféré choisir parmi des sujets en raison de sa grande importance dans la résolution de problèmes mathématiques très anciens qui restaient ouverts malgré le développement scientifique et mathématique à l'heure actuelle, Nous avons essayé autant que possible et détaillé les éléments du sujet, et en conséquence, nous n'avons pas abordé la petite partie de celui-ci, Nous espérons que cette recherche profitera particulièrement à de nombreux future chercheurs intéressés à étudier ce sujet important et intéressant et qu'elle recevra une grande attention afin de se débarrasser des problèmes en suspens et d'y trouver des solutions décisives.

Bibliographie

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

[2] J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London. Math. Soc. vol. 1 (1), 193-291, 1966.

[3] L.E. Dickson, History of the theory of numbers, Vol. II, Diophantine analysis, Dover Publications, New York, 2005.

[4] Husemöller, D. (1987). Elliptic curves, volume 111 of. Graduate Texts in Mathematics, 99.

[5] C. G. J. Jacobi, De usu theoriae integralium ellipticorum et integralium Abelianorum in analysi Diophantea. Journal für die reine und angewandte Mathematik, 1835(13), 353-355.

[6] L.J. Mordell, Diophantine Equations, Pure and Applied Mathematics, vol. 30 (Academic, London, 1969).

[7] C.L. Siegel, The integer solutions of the equation $y^2 = an^n + bx^(n-1) + \cdots + k$. J. Lond. Math. Soc. (2) 1, 66–68 (1926).

[8] C.L. Siegel, ¨ Uber einige Anwendungen diophantischer Approximationen (1929), in Collected Works (Springer, 1966), pp. 209–266.

[9] J.H. Silverman, Advanced topics in the arithmetic of elliptic curves, Vol 151, Springer Science and Business Media, 2013.

[10] J.H. Silverman, Integer points and the rank of elliptic curves. Invent. Math. 66(3), 395–404 (1982).

[11] Silverman, J. H. and Tate, J. T. (1992). Rational points on elliptic curves (Vol. 9). New York : Springer-Verlag.

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

[13] J. T. Tate, *The arithmetic of elliptic curves*, Invent. Math. vol. 23 (3-4), 179-206, 1974.

[14] S.Tengely, M. Ulas, (2017). On certain Diophantine equations of the form z2= f (x) 2±g (y) 2. Journal of Number Theory, 174, 239-257.

[15] M. Ulas, A. Togbé, On the Diophantine equation $z^2 = f(x)^2 \pm f(y)^2$. Publ. Math. Debrecen 76(1-2), 183–201 (2010).

[16] A. E. A. Youmbai and D. Behloul, Rational solutions of the diophantine equations $f(x)^2 \pm f(y)^2 = z^2$, Periodica Mathematica Hungarica 79 , no. 2, 255-260, 2019.

[17] Y. Zhang, A. S. Zargar. "On the Diophantine equations $z^2 = f(x)^2 \pm f(y)^2$ involving quartic polynomials." Periodica Mathematica Hungarica 79, no. 1 (2019) : 25-31.

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

Résumé

Dans ce mémoire, nous étudions quelques équations diophantiennes qui ont un rapport directe avec la théorie des courbes elliptiques. Pour la résolution de ces problèmes, on se ramène à modifier les variables d'une manière appropriée qui permet de les convertir en équations pouvant être résolues en utilisant la théorie des les courbes elliptiques où dans chaque cas nous montrons que la courbe elliptique est de rang strictement positif (possède un points d'ordre infini).

Mots clés : Courbes Elliptiques - Nombre Congruent - Somme se carrés - Solutions Rationnelles.

Abstract

In this thesis, we study some diophantine equations that have a direct relation with the theory of elliptic curves. For the resolution of these problems, we come back to modify the variables in an appropriate way that allows to convert them into equations that can be solved using the theory of elliptic curves where in each case we show that the elliptic curve has a strictly positive rank (has points of infinite order).

ملخص الدرَاسة

في هذه المذكرة ، قمنَا بدرَاسة بعض المعَادلَات الديوفنتية التي لهَا علَاقة مبَاشرة بنظرية المنحنيَات النَاقصية لحل هذه المسَائل قمنَا بتعديل المتغيرَات بطريقة مِنَاسبة تسمح بتحويلهَا إِلَى معَادلَات يمكن حلهَا بطريقة المنحنيَات النَاقصية حيث نظهر في كل حَالة أَن ترتيب المنحنَى النَاقصي موجب تمَامًا (له نقطة ذَات رتبة غير متنهية)