école normale supérieure rennes

UNIVERSITÉ DE RENNES 1

Mémoire pour le Master 2
Leçon 124 - Exemples d'équations diophantiennes

Emeline LUIRARD

Année 2017-2018

Table des matières

Introduction

Diophante d'Alexandrie, vers les années 250 de notre ère, a été le premier à rechercher systématiquement les solutions en nombres entiers, ou rationnels, d'une équation ou d'un système d'équations polynomiales à coefficients entiers. Souvent, le problème s'écrit simplement mais la résolution peut être complexe. Gauss disait de la théorie des nombres que "son charme particulier vient de la simplicité des énoncés jointe à la difficulté des preuves". En effet, on a démontré que le dixième problème de Hilbert a une réponse négative : il n'existe pas d'algorithme universel permettant de décider si une équation diophantienne a une solution en nombre entiers, c'est le théorème de Matiyasevich (J. Robinson, Yu. V. Matijasevic, 1970).

Pour illustrer la difficulté des preuves par rapport aux énoncés, on peut rappeler que les équations de Fermat ont demandé plusieurs siècles de recherches avant d'être résolues. En effet, le dernier théorème de Fermat n'a été démontré qu'en 1994 par Wiles, après plus de 300 ans de recherches.

Pierre de Fermat consacre beaucoup de ses recherches à la résolution de questions diophantiennes. Il énonca le théorème : Soit $n \geq 3$ un entier. Les solutions de $x^n + y^n = z^n$, où x, y et z sont des entiers, vérifient toutes $xyz = 0$. C'est ce qu'on appelle le dernier théorème de Fermat. Fermat lui-même a résolut le cas $n = 4$, en utilisant la méthode de la descente infinie.Ensuite, c'est Euler, qui un siècle plus tard, a démontré le cas $n = 3$ en utilisant les entiers d'Eisenstein. Il y a eu d'autres preuves pour des n particuliers. Mais il a fallu attendre 1994, et le mathématicien anglais Andrew Wiles, pour trouver une réponse définitive : Fermat avait raison !

Un autre personnage important dans le monde des équations diophantiennes est Joseph-Louis Lagrange qui généralisa des équations diophantiennes déjà traitées. Par exemple, le problème des deux carrés devient l'équation $x^2 + ny^2 = p$, où p est un nombre premier, et n un entier sans facteur carré. Afin de résoudre cette équation, il étudie les formes quadratiques binaires, et notamment une

relation d'équivalence sur celles-ci. Il s'est aussi intéressé à un autre problème : savoir le nombre minimal n de carrés nécessaires pour écrire tout nombre comme une somme de n carrés. Cela donna la théorème des quatre carrés de Lagrange.

Gauss est encore une autre personnalité qui est apparue dans le paysage des équations diophantiennes. Il proposa l'usage des anneaux euclidiens et les anneaux d'entiers algèbriques pour venir à bout des équations diophantiennes. Cependant lorsque les anneaux ne sont pas factoriels, il n'y a pas unicité dans la décomposition en facteurs premiers. Cela posa problème et Ernst Kummer interprèta ce problème comme un défaut de nombres premiers : c'est parce qu'il en manque que l'unicité de la décomposition disparaît. Son idée est alors de rajouter des nouveaux nombres : les nombres idéaux. Richard Dedekind formalise ces nouveaux nombres par le concept que l'on connaît aujourd'hui, celui d'idéal. On obtient alors la propriété suivante : tout idéal se décompose de manière unique en un produit d'idéaux premiers. Ainsi, la recherche de résolution d'équations diophantiennes a permis d'introduire de nouveaux objets et donc de créer de nouvelles branches de recherches en mathématiques.

Définition 0.1. Une *équation diophantienne* est une équation de la forme $P(x_1, \dots, x_n) = 0$ d'inconnues $x_1, \dots, x_n$, où $P \in \mathbb{Z}[X]$.

1 Equations du premier degré

1.1 En deux variables

On commence par un cas simple : le cas à deux variables. On veut résoudre l'équation $ax+by = c$, où $a, b \in \mathbb{Z}\backslash\{0\}$ et $c \in \mathbb{Z}$. On a une condition nécessaire et suffisante pour l'existence des solutions, ainsi que la forme de celles-ci.

Théorème 1.1. *Soient $a, b \in \mathbb{Z}\backslash\{0\}$ et $c \in \mathbb{Z}$. On note $d = pgcd(a, b)$.*
- *Si $d \nmid c$, alors l'équation $ax + by = c$ n'a pas de solutions dans $\mathbb{Z}$.*
- *Sinon, l'ensemble des solutions est donné par $\left\{\left(x_0 + \dfrac{bk}{d},\ y_0 - \dfrac{ak}{d}\right),\ k \in \mathbb{Z}\right\}$, où (x_0, y_0) est une solution particulière.*

Démonstration. Soit (x, y) une solution, alors $d \mid ax + by = c$. Donc, si $d \nmid c$, l'équation $ax + by = c$ n'a pas de solutions dans $\mathbb{Z}$.
Supposons maintenant que d divise c et supposons connue une solution particulière $ax_0 + by_0 = c$. On a alors $a(x - x_0) = -b(y - y_0)$. Donc en posant $a' = \frac{a}{d}$ et $b' = \frac{b}{d}$, on obtient $a'(x - x_0) = -b'(y - y_0)$, avec a' et b' premiers entre eux. Ainsi, d'après le lemme de Gauss, $a' \mid y - y_0$, i.e. il existe $k \in \mathbb{Z}$ tel que $y = y_0 - a'k$. En remplaçant dans l'équation, on obtient $x = b'k + x_0$. On peut vérifier alors que les couples de cette forme sont bien solutions. □

Exemple 1.1. L'ensemble des solutions de $3x+7y = 11$ est donné par $\{(6 + 7k,\ -1 - 3k),\ k \in \mathbb{Z}\}$.

Exemple 1.2. L'équation $303x + 57y = a^2 + 1$ n'a pas de solutions dans $\mathbb{Z}$ pour $a \in \mathbb{Z}$. En effet, $pgcd(303, 57) = 3$ or $3 \nmid a^2 + 1$.

1.2 En n variables

On passe maintenant au cas général, on cherche les solutions de l'équation $a_1x_1+\cdots+a_nx_n = b$ où $a_1, \dots, a_n \in \mathbb{Z}\backslash\{0\}$ et $b \in \mathbb{Z}$. On a, à nouveau, une condition nécessaire et suffisante pour l'existence des solutions, ainsi que la forme de celles-ci.

Théorème 1.2. *Soient $a_1, \dots, a_n \in \mathbb{Z}\backslash\{0\}$ et $b \in \mathbb{Z}$. On note $d = pgcd(a_1, \dots, a_n)$.*
- *Si $d \nmid b$, alors l'équation $a_1x_1 + \cdots + a_nx_n = b$ n'a pas de solutions dans $\mathbb{Z}$.*

— *Sinon, l'ensemble des solutions est donné par* $\left\{\frac{b}{d}V_1 + k_1V_2 + \cdots + k_{n-1}V_n,\ k_1, \ldots, k_{n-1} \in \mathbb{Z}\right\}$, *où les* V_i *sont les colonnes de* $V \in \mathrm{GL}_n(\mathbb{Z})$, *qui vérifie* $(a_1, \ldots, a_n)V = (d, 0, \ldots, 0)$.

Démonstration. L'idée est de réécrire l'équation diophantienne sous la forme d'un problème matriciel :

$$(a_1, \ldots, a_n)\ {}^t(x_1, \ldots, x_n) = (b).$$

Par des opérations élémentaires sur la matrice $A = (a_1, \ldots, a_n)$, on se ramène à une matrice de la forme $(d, 0, \ldots, 0)$, c'est la forme normale de Smith. En fait, dans des notations évidentes, $Ax = b$ se réécrit $AVy = b$ où $x = Vy$, avec V la matrice des opérations élémentaires de la mise sous forme échelonnée. On a donc $AV = (d, 0, \ldots, 0)$ et l'équation $AVy = b$ se résout facilement, puis on remonte à x grâce à la relation $x = Vy$. □

Exemple 1.3. Considérons l'équation $3x + 4y + 7z = b$, où $b \in \mathbb{Z}$. On a $d = 1$ et par exemple $V = \begin{pmatrix} -1 & 4 & -1 \\ 1 & -3 & -1 \\ 0 & 0 & 1 \end{pmatrix}$, en utilisant la méthode de la preuve. Alors l'ensemble des solutions est $\{(-b + 4k - l,\ b - 3k - l,\ l),\ (k, l) \in \mathbb{Z}^2\}$.

1.3 Un exemple : le problème de Frobenius ou problème des pièces de monnaie

On considère $r \geq 2$ pièces de monnaies de valeur $0 < a_1 < \cdots < a_r$, où $a_1, \ldots, a_r$ sont des entiers premiers entre eux dans leur ensemble. Le problème de Frobenius consiste à déterminer le montant maximal N qu'on ne peut pas obtenir avec ces pièces. On appelle ce nombre, le *nombre de Frobenius*. Mathématiquement, on cherche N, qui vérifie :

— pour tout $n > N$, il existe $x_1, \ldots, x_n \in \mathbb{N}$ tels que $n = a_1x_1 + \ldots a_rx_r$,

— N n'est pas combinaison linéaire entière de $a_1, \ldots, a_r$.

Commençons par donner un équivalent du nombre de solutions de l'équation $a_1x_1 + \cdots + a_rx_r = n$, lorsque n tend vers l'infini.

Proposition 1.1 (Entiers à parts fixés)**.** *Soient* $a_1, \ldots, a_r \in \mathbb{N}\backslash\{0\}$ *premiers entre eux dans leur ensemble. On note, pour* $n \in \mathbb{N}$, $U_n = \#\{(x_1, \ldots, x_r) \in \mathbb{N}^r,\ a_1x_1 + \cdots + a_rx_r = n\}$. *Alors*

$$U_n \sim \frac{1}{a_1 \ldots a_r} \frac{n^{r-1}}{(r-1)!}.$$

Etant donné que le membre de droite tend vers l'infini lorsque n tend vers l'infini, on déduit de la proposition précédente le corollaire suivant.

Corollaire 1.3. *Pour tout* $r \geq 2$, *le nombre de Frobenius existe.*

Proposition 1.2. *Pour* $r = 2$, *le nombre de Frobenius est explicite et donné par* $N = a_1a_2 - a_1 - a_2$.

Démonstration. Soient a et b premiers entre eux. Notons $M = \{ax + by,\ x, y \in \mathbb{N}\}$. Soit $m \in \mathbb{N}$. D'après le théorème de Bézout, on sait qu'il existe u, $v \in \mathbb{Z}$ tels que $au + bv = m$. Quitte a remplacer u par son reste modulo b, on peut supposer que $0 \leq u \leq b - 1$.
Si $m \notin M$, alors $v \leq -1$. Ainsi, $m = au + bv \leq ab - a - b$. Donc si $m > ab - a - b$, alors $m \in M$.
Supposons maintenant qu'il existe $x, y \in \mathbb{N}$ tels que $ax + by = ab - a - b$. Alors $a(x+1) = b(a-1-y)$, d'où d'après le lemme de Gauss, $a \mid 1 + y$ et donc $a \leq 1 + y$. Ainsi $0 \geq b(a - 1 - y) = (x + 1)a < 0$. C'est absurde, donc $ab - a - b \notin M$. Le nombre de Frobenius est donc $ab - a - b$. □

Remarque. En général, il n'existe pas de formule explicite pour le nombre de Frobenius.

Exemple 1.4. On considère des pièces de monnaie de 5 et 7 centimes. D'après la formule de la proposition précédente, $N = 23$. En fait, les nombres inférieurs à 23 qui peuvent se décomposer en pièces de 5 et de 7 sont : 5, 7, 10, 12, 14, 15, 17, 19, 20, 21, 22.

Remarque. On peut montrer que parmi les entiers plus petit que le nombre de Frobenius, il n'y en a qu'un sur deux qui est représentable. Voir...

1.4 Systèmes modulaires

On s'intéresse maintenant à la résolution d'équations diophantiennes linéaires sous forme de systèmes linéaires. On a le théorème d'existence de solutions suivant

Théorème 1.4 (Théorème chinois)**.** *Soient $m_1, \dots, m_p \in \mathbb{Z}$ premiers entre eux deux à deux. Pour tout $a_1, \dots, a_p \in \mathbb{Z}$, il existe une unique solution modulo $m_1 \dots m_p$ au système*

$$\begin{cases} x \equiv a_1[m_1] \\ \dots \\ x \equiv a_p[m_p]. \end{cases} \tag{1}$$

Pour déterminer cette solution, on utilise la méthode de Newton : On cherche x sous la forme $x = \gamma_1 + \gamma_2 m_1 + \gamma_3(m_1 m_2) + \dots + \gamma_p(m_1 \dots m_{p-1})$. Puis on calcule dans l'ordre les coefficients $\gamma_1, \dots, \gamma_p$, que l'on choisira minimaux. Donnons un exemple pour comprendre.

Exemple 1.5. On considère le système

$$\begin{cases} x \equiv 2[4] \\ x \equiv 3[5] \\ x \equiv 1[9]. \end{cases} \tag{2}$$

Comme 4, 5 et 9 sont premiers entre eux deux à deux, on sait qu'il existe une unique solution modulo $4 \times 5 \times 9 = 180$. On pose $x = \gamma_1 + \gamma_2 4 + \gamma_3(4 \times 5)$ On a $\gamma_1 \equiv 2[4]$ donc on choisit $\gamma_1 = 2$. Puis, $\gamma_1 + \gamma_2 4 \equiv 3[5]$, d'où $\gamma_2 4 \equiv 1[5]$, ainsi $\gamma_2 \equiv -1[5]$ car l'inverse de 4 modulo 5 est -1. On prend donc $\gamma_2 = -1$. Enfin, $2 - 4 + \gamma_3 20 \equiv 1[9]$ d'où $2\gamma_3 \equiv 3[9]$ et donc $\gamma_3 \equiv -3[9]$ car l'inverse de 2 modulo 9 est 5. On prend donc $\gamma_3 = -3$. Donc $x = -62$.
Donc l'ensemble des solutions de 2 est $\{-62 + 180k,\ k \in \mathbb{Z}\}$.

2 Méthodes et exemples

Maintenant qu'on a vu la résolution d'équations diophantiennes "simples", on aimerait s'attaquer à des problèmes diophantiens plus "costauds". On s'intéresse donc aux méthodes de résolution.

2.1 Réduction modulaire

Idée : Lorsque les coefficients de P sont multiples d'un nombre a, on étudie $P(x_1, \dots, x_n) = 0$ dans $\mathbb{F}_a$. S'il n'y a pas de solutions dans $\mathbb{F}_a$ alors il n'y a pas de solutions sur $\mathbb{Z}$. Regardons des exemples pour comprendre.

Exemple 2.1. L'équation $x^2 + y^2 = 4z + 7$ n'a pas de solutions entières. En effet, si (x, y, z) est une solution, alors $x^2 + y^2 \equiv 3[4]$, or les carrés modulo 4 sont 0 et 1, c'est donc impossible.

Exemple 2.2. L'équation $x^3 + 5 = 117y^3$ n'a pas de solutions entières. En effet, si (x, y) est une solution, alors $x^3 \equiv 4[9]$, or les cubes modulo 9 sont 0, 1 et -1, c'est donc impossible.
Pour la même raison, l'équation $x^3 + y^3 + z^3 = 4$ n'a pas de solutions entières.

2.2 Descente infinie de Fermat

Dans ce paragraphe, on explique la méthode de Pierre de Fermat : la méthode de la descente infinie. Considérons une équation diophantienne. On veut montrer qu'elle n'a que des solutions non triviales.
On suppose qu'il existe une solution non triviale, on choisit des conditions de minimalité sur cette solution. Puis on construit une solution non triviale qui est plus petite que la première. On aboutit alors à une contradiction.
Il est plus simple de voir la méthode sur un exemple pour comprendre.

Exemple 2.3. L'équation $x^3 + 2y^3 = 4z^3$ n'a pas d'autres solutions entières que $(0, 0, 0)$.
On va donc utiliser la méthode de la descente infinie de Fermat. Supposons que cette équation diophantienne possède des solutions. Soit $x = x_0$ la valeur qui correspond à la plus petite valeur positive de x pour laquelle cette équation possède une solution. Soit donc (x_0, y_0, z_0) une telle solution. Alors on a $x_0^3 + 2y_0^3 = 4z_0^3$. Ainsi, $2 \mid x_0^3$ donc $2 \mid x_0$ donc il existe un entier positif a tel que $x_0 = 2a$. L'équation se réécrit donc sous la forme $8a^3 + 2y_0^3 = 4z_0^3$, c'est à dire $4a^3 + y_0^3 = 2z_0^3$. Ainsi, $2 \mid y_0$, d'où il existe b tel que $y_0 = 2b$. L'équation se réécrit alors $4a^3 + 8b^3 = 2z_0^3$, c'est à dire $2a^3 + 4b^3 = z_0^3$. Ainsi, à nouveau, $2 \mid z_0$, d'où il existe c tel que $z_0 = 2c$. L'équation se réécrit alors $2a^3 + 4b^3 = 8c^3$, ou encore, $a^3 + 2b^3 = 4c^3$. Ainsi (a, b, c) est un triplet solution de l'équation de départ, mais $0 < a < x_0$, ce qui contredit la minimalité de x_0 et fournit une absurdité.

On s'intéresse maintenant à l'équation de Fermat $x^n + y^n = z^n$, pour $n \geq 1$. Fermat a énoncé que cette équation n'admet pas de solution vérifiant $xyz \neq 0$, pour $n \geq 3$. Commençons par remarquer qu'on peut se ramener au cas où n est premier. En effet, si on n'a pas de telle solution pour p premier alors il n'y en a pas pour tout n multiple de p. Cependant, on va montrer qu'il existe des solutions pour $n = 2$, il va donc falloir étudier la cas $n = 4$ afin de régler le cas des puissances de deux qui s'écrivent 4×2^k. Nous ne ferons pas la démonstration pour n quelconque, celle-ci a nécessité plus de 300 ans de recherches, avant d'être démontrée par André Wiles en 1994 !

Remarquons aussi que, si (x, y, z) est solution de $x^n + y^n = z^n$, pour $n \in \mathbb{N}$ alors, en posant $d = pgcd(x, y, z)$, on a $x'^n + y'^n = z'^n$, où $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$ sont premiers entre eux. Ainsi, on se restreint à l'étude de solutions dites primitives.

Théorème 2.1. *Les solutions de l'équation $x^2 + y^2 = z^2$, avec x, y et z premiers entre eux, sont données, à une permutation de x et y près, par :*

$$\begin{cases} x = u^2 - v^2, \\ y = 2uv, \\ z = u^2 + v^2, \end{cases} \tag{3}$$

avec $u, v \in \mathbb{Z}$, premiers entre eux, de parité différente.

Démonstration.
- Soit (x, y, z) une solution.
  - ◇ Commençons par remarquer que si un nombre premier p divise deux des trois nombres, alors il divise le dernier. Ainsi x, y, z sont premiers entre deux à deux.
  - ◇ Si x et y sont impairs, alors $x \equiv 1, 3[4]$ et $y \equiv 1, 3[4]$, donc $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$, ainsi $z^2 \equiv 2[4]$. Ceci est impossible car les carrés modulo 4 sont 0 et 1. Donc l'un des deux nombres est pair. Disons y est pair.
  - ◇ Si x est pair, cela contredit le fait que $pgcd(x, y) = 1$, ainsi x est impair. Comme x est impair et y est pair, z ne peut pas être pair car $pgcd(y, z) = 1$ donc z est impair.
  - ◇ L'équation de Fermat se réécrit $z^2 - x^2 = y^2$ ou encore $(z - x)(z + x) = y^2$. L'idée, maintenant, est de chercher les facteurs premiers communs à $z + x$ et $z - x$.
    On a montré que x et z sont impairs, ainsi, $2 \mid (x + z)$ et $2 \mid (z - x)$.
    Soit, maintenant, $p \neq 2$ premier tel que $p \mid (z+x)$ et $p \mid (z-x)$. Alors $p \mid (x + z) + (z - x) = 2z$ et $p \mid (x + z) - (z - x) = 2x$. Comme p est premier impair, d'après le lemme de Gauss, on a $p \mid z$ et $p \mid x$. C'est impossible puisque x et z sont premiers entre eux.
    On en déduit donc que $pgcd(z + x, z - x) = 2$, et ainsi, il existe $a, b \in \mathbb{Z}$ premiers entre eux tels que $z + x = 2a$ et $z - x = 2b$. Donc $y^2 = 4ab$, ce qui se réécrit, (rappelons que y est pair), $(\frac{y}{2})^2 = ab$.
  - ◇ La décomposition de $(\frac{y}{2})^2$ en facteurs premiers ne présente que des exposants pairs. Comme, de plus, $pgcd(a, b) = 1$, les mêmes facteurs se retrouvent soit dans a soit dans b, ainsi la décomposition en facteurs premiers de a et de b n'a que des exposants pairs. Il existe donc $u, v \in \mathbb{N}$ premiers entre eux (puisque a et b le sont) vérifiant $a = u^2$ et $b = v^2$. Ainsi, $z + x = 2a = 2u^2$, $z - x = 2b = 2v^2$ et donc $z = u^2 + v^2$, $x = u^2 - v^2$ et $y = 2uv$. Comme z est impair, u et v sont de parité différente.

- Réciproquement, si on a $x = u^2 - v^2$, $y = 2uv$ et $z = u^2 + v^2$, avec $u,\ v\ \in \mathbb{Z}$, premiers entre eux et de parité différente, alors $x^2+y^2 = z^2$. En outre, si 2 divise x, y et z, alors en particulier $u^2 \equiv v^2[2]$, ce qui contredit le fait que u et v sont de parité différente. Si $p \neq 2$ premier divise x, y et z, alors $p \mid (u^2-v^2)$ et $p \mid (u^2+v^2)$ d'où $p \mid 2u^2$ et $p \mid 2v^2$, ce qui implique par lemme de Gauss que $p \mid u^2$ et $p \mid v^2$. Comme p est premier, on obtient $p \mid u$ et $p \mid v$, ce qui est impossible puisque u et v sont premiers entre eux.

□

A partir de ce théorème, on peut maintenant démontrer le dernier théorème de Fermat pour $n = 4$.

Théorème 2.2. *L'équation diophantienne $x^4 + y^4 = z^4$ n'admet pas de solution vérifiant $xyz \neq 0$.*

Démonstration. D'après la remarque du début, on se restreint à la recherche de solutions primitives. On va utiliser l'idée de Fermat, lui-même. Remarquons que si (x, y, z) est une solution primitive de $x^4+y^4 = z^4$ avec x, y, z premiers entre eux, alors (x, y, z^2) est une solution primitive de $x^4+y^4 = w^2$ avec $w = z^2$. Il suffit donc de montrer que $x^4+y^4 = z^2$ n'a pas de solution primitive vérifiant $xyz \neq 0$. Pour cela, nous allons utiliser la méthode de la descente infinie. Supposons qu'il y ait une telle solution. Soit (x, y, z) un couple solution avec $z > 0$ et z minimal. Comme pour le théorème précédent, $x,\ y,\ z$ sont premiers entre eux dans leur ensemble donc premiers entre eux deux à deux.

- ◇ On peut refaire les deux premières étapes de la démonstration précédente, ce qui montre que x et z sont impairs et y est pair.
- ◇ Remarquons ensuite que l'équation $x^4 + y^4 = z^2$ se réécrit $(x^2)^2 + (y^2)^2 = z^2$ avec x^2, y^2, z premiers entre eux. Donc, par Théorème 2.1, il existe $u, v \in \mathbb{Z}$ premiers entre eux, de parité différente, tels que $x^2 = u^2 - v^2$, $y^2 = 2uv$ et $z = u^2 + v^2$ (car c'est y^2 qui est pair). Ainsi, on obtient $x^2 + v^2 = u^2$.
- ◇ Comme u et v sont premiers entre eux, x, u et v sont premiers entre eux. De plus, par la même méthode que précédemment, on montre que x et v ne peuvent être tous les deux impairs. Or x est impair, ainsi v est pair et u est impair.
- ◇ On peut donc à nouveau appliquer le Théorème 2.1 : il existe $a, b \in \mathbb{Z}$ premiers entre eux, de parité différente tels que $x = a^2 - b^2$, $v = 2ab$ et $u = a^2 + b^2$ (car c'est v qui est pair). Donc $y^2 = 2uv = 4ab(a^2 + b^2)$.
- ◇ La décomposition de $(\frac{y}{2})^2$ en facteurs premiers ne présente que des exposants pairs. Comme a, b et $a^2 + b^2$ sont premiers entre eux, les mêmes facteurs se retrouvent soit dans a, soit dans b, soit dans $a^2 + b^2$, ainsi la décomposition en facteurs premiers de a, b et $a^2 + b^2$ n'a que des exposants pairs. Ainsi, il existe $\alpha,\ \beta,\ \gamma \in \mathbb{N}$ premiers entre eux tels que $a = \alpha^2$, $b = \beta^2$ et $a^2 + b^2 = \gamma^2$.
  Donc $\gamma^2 = a^2 + b^2 = \alpha^4 + \beta^4$, ainsi (α, β, γ) est une solution primitive, or $0 < \gamma \leq \gamma^2 = u < z$ (la première inégalité vient du fait que $(a, b) \neq (0, 0)$ puisqu'on a choisi une solution non triviale, la dernière vient du fait que $v \neq 0$ sinon $x^2 = z$ et cela contredit $pgcd(x, z) = 1$). Ceci contredit la minimalité de z et donc conclut la preuve du théorème.

□

2.3 Utilisation des corps quadratiques

Il s'avère qu'on peut aussi utiliser les corps quadratiques afin de résoudre des équations diophantiennes. Nous allons en voir quelques exemples dans cette partie et dans la suite. Soit $d \in \mathbb{Z}$ sans facteur carré.

Définition 2.1. On définit $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{C},\ a, b \in \mathbb{Q}\}$, avec pour convention, si $d < 0$, $\sqrt{d} = \mathrm{i}\sqrt{|d|}$. C'est un sous corps de $\mathbb{C}$ contenant $\mathbb{Q}$. On dit que c'est un *corps de nombres quadratiques*.

Définition 2.2. On définit l'application

$$\begin{array}{rccc} N & : & \mathbb{Q}[\sqrt{d}] & \to & \mathbb{Q} \\ & & a + b\sqrt{d} & \mapsto & a^2 - db^2. \end{array}$$

Définition 2.3. On dit que $x \in \mathbb{Q}[\sqrt{d}]$ est un *entier quadratique* de $\mathbb{Q}[\sqrt{d}]$ si x est racine d'un polynôme à coefficients dans $\mathbb{Z}$, de degré 2. Si $\mathbb{K} = \mathbb{Q}[\sqrt{d}]$, on note $\mathbb{A}_{\mathbb{K}}$ *l'ensemble des entiers quadratiques de* $\mathbb{K}$. C'est un sous-anneau de $\mathbb{K}$.

Exemple 2.4. Le nombre d'or $\dfrac{1+\sqrt{5}}{2} \in \mathbb{Q}[\sqrt{5}]$ est un entier quadratique : il est racine de X^2-X-1.

On s'intéresse maintenant à deux anneaux d'entiers quadratiques : les entiers de Gauss et les entiers d'Eisenstein. Ces deux anneaux sont intéressants puisqu'ils sont euclidiens (et donc factoriels), ainsi la décomposition en facteurs premiers y est unique. Cette propriété n'est pas vraie sur tous les anneaux d'entiers quadratiques, c'est ce qui a posé problème pour la résolution d'équations diophantiennes. Pour cette raison, Kummer a dit qu'il manquait des nombres premiers, il a donc inventé les nombres idéaux, que l'on appelle aujourd'hui idéaux. Ceux-ci vérifient la propriété que tout idéal d'un anneau d'entiers quadratiques s'écrit de manière unique comme produit d'idéaux premiers.

2.3.1 Entiers de Gauss

Définition 2.4. On définit l'ensemble des *entiers de Gauss* par $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b,\ a, b \in \mathbb{Z}\}$. C'est l'anneau des entiers quadratiques de $\mathbb{Q}[\mathrm{i}]$.

Comme annoncé, nous avons la proposition suivante.

Proposition 2.1. *L'anneau des entiers de Gauss munit du stathme N est euclidien.*

Démonstration. Soient $z, t \in \mathbb{Z}[\mathrm{i}]\backslash\{0\}$. On a $z/t \in \mathbb{C}$ est de la forme $z/t = x + \mathrm{i}y$.
On veut approximer $\frac{z}{t}$ par un entier de Gauss $q = a + \mathrm{i}b$ où a et b sont les plus proches entiers de x et y respectivement. On peut choisir a et b tels que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$. Ainsi,

$$\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1.$$

On pose alors $r = z - qt$, on a $r \in \mathbb{Z}[\mathrm{i}]$, car z, q et t sont dans $\mathbb{Z}[\mathrm{i}]$. Et on a $r = t\left(\frac{z}{t} - q\right)$ ainsi

$$|r| = |t|\left|\frac{z}{t} - q\right| < |t|, \quad \text{et en élevant au carré,} \quad N(r) < N(t).$$

On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$. □

On connait les inversibles de cet anneau, ce qui nous servira pour la suite.

Proposition 2.2. *Les inversibles de $\mathbb{Z}[i]$ sont $-i, i, -1, 1$.*

Démonstration. Il est clair que $-\mathrm{i}, \mathrm{i}, -1, 1$ sont inversibles dans $\mathbb{Z}[\mathrm{i}]$.
Si $z = a + \mathrm{i}b \in \mathbb{Z}[\mathrm{i}]^*$, il existe $z' \in \mathbb{Z}[\mathrm{i}]^*$ tel que $zz' = 1$, d'où $N(z)N(z') = 1$. Ainsi, $N(z) = 1$ d'où $a^2 + b^2 = 1$ et donc ($a = 0$ et $b = \pm 1$) ou ($a = \pm 1$ et $b = 0$). □

Voyons donc une première utilisation des entiers de Gauss pour la résolution d'équation diophantienne.

Exemple 2.5. Etudions un cas particulier de l'équation de Mordell : on considère l'équation $y^2 = x^3 - 1$.
Soit (x, y, z) une solution. On remarque d'abord que x est impair sinon $y^2 \equiv -1[4]$, ce qui est impossible puisque les carrés modulo 4 sont 0 et 1. L'idée est de factoriser dans $\mathbb{Z}[\mathrm{i}]$, qui est euclidien donc factoriel. On a $(y + \mathrm{i})(y - \mathrm{i}) = x^3$.
Montrons que $y+\mathrm{i}$ et $y-\mathrm{i}$ sont premiers entre eux. Supposons que $p \in \mathbb{Z}[\mathrm{i}]$, premier dans $\mathbb{Z}[\mathrm{i}]$, divise $y+\mathrm{i}$ et $y-\mathrm{i}$. Alors p divise leur différence $2\mathrm{i}$. Donc en utilisant l'application N, $N(p) \mid 4$. Comme p n'est pas inversible, on obtient $N(p) \in \{2, 4\}$. Cependant, $p \mid (y+\mathrm{i})$ d'où $N(p) \mid N(y+\mathrm{i}) = y^2+1 = x^3$ dans $\mathbb{Z}$. C'est impossible car x est impair. Donc $y+\mathrm{i}$ et $y-\mathrm{i}$ n'ont aucun facteur premier en commun. Comme

tous les facteurs premiers figurant dans x^3 sont des cubes, d'après l'unicité de la décomposition en facteurs premiers (à un inversible près) dans un anneau factoriel, $y + \mathrm{i} = \epsilon(p_1 \dots p_k)^3$ avec $\epsilon \in \mathbb{Z}[\mathrm{i}]^\times$. Cependant tout élément inversible est un cube dans $\mathbb{Z}[\mathrm{i}]$: $1 = 1^3$, $-1 = (-1)^3$, $\mathrm{i} = (-\mathrm{i})^3$ et $-\mathrm{i} = \mathrm{i}^3$. Donc $y + \mathrm{i} = (a + \mathrm{i}b)^3$, avec $a, b \in \mathbb{Z}$. En développant, on obtient $y = a^3 - 3ab2$ et $1 = 3a^2b - b3$. Ainsi $b \mid 1$ d'où $b = \pm 1$ et donc $\pm 1 = 3a^2 - 1$. Donc $b = -1$ et $a = 0$, ainsi $y = 0$ et $x^3 = 1$, donc $x = 1$. L'équation a donc pour unique solution $(x = 1, y = 0)$.

2.3.2 Entiers d'Eisenstein

Définition 2.5. On définit l'ensemble des *entiers d'Eisenstein* par $\mathbb{Z}[j] = \{a + jb,\ a, b \in \mathbb{Z}\}$, où $j = \dfrac{1 + \mathrm{i}\sqrt{3}}{2}$. C'est l'anneau des entiers quadratiques de $\mathbb{Q}[\mathrm{i}\sqrt{3}]$.

Comme énoncé au par avant, nous avons la propriété suivante.

Proposition 2.3. *L'anneau des entiers d'Eisenstein munit du stathme N est euclidien.*

La connaissance des inversibles de cet anneau nous sera également utile.

Proposition 2.4. *Les inversibles de $\mathbb{Z}[j]$ sont $-1, 1, \bar{j}, j, -j, -\bar{j}$.*

Exemple 2.6. Grâce à cet anneau, on peut montrer le théorème de Fermat pour $n = 3$: l'équation $x^3 + y^3 = z^3$ n'admet pas de solutions entières vérifiant $xyz \neq 0$. On renvoit à [1, Section 5.7 p.57] pour la preuve.

3 Carrés

Maintenant que nous avons des méthodes plus générales, compliquons les problèmes diophantiens en augmentant le degré.

3.1 Symbole de Legendre

On va commencer par introduire un outil qui va nous être utile par la suite : le symbole de Legendre.
Soit p un nombre premier.

Définition 3.1. On définit le *symbole de Legendre*, pour $n \in \mathbb{Z}$, par

$$\left(\frac{n}{p}\right) = \begin{cases} 0, \text{ si } n \equiv 0[p] \\ 1, \text{ si } n \text{ est un carré mod } p \\ -1, \text{ si } n \text{ n'est pas un carré mod } p. \end{cases} \tag{4}$$

Ce symbole va nous permettre de savoir assez facilement quels sont les carrés dans les corps finis.

Exemple 3.1. On a $\left(\dfrac{2}{7}\right) = 1$ et $\left(\dfrac{3}{7}\right) = -1$

Le critère d'Euler donne un moyen efficace de calculer ce symbole lorsque p est petit.

Proposition 3.1 (Critère d'Euler)**.** *Si $p \neq 2$,* $\left(\dfrac{n}{p}\right) \equiv n^{\frac{p-1}{2}}[p]$.

Le symbole de Legendre est un morphisme multiplicatif :

Proposition 3.2. *Pour tout $n, m \in \mathbb{Z}$,* $\left(\dfrac{mn}{p}\right) = \left(\dfrac{m}{p}\right)\left(\dfrac{n}{p}\right)$.

Ainsi, sur un corps fini, le produit de deux carrés est un carré et même le produit de deux non-carrés est un carré. Ce qui n'est pas le cas sur tous les corps infinis : par exemple $6 = 2 \times 3$ n'est pas un carré dans $\mathbb{N}$ et pourtant 2 et 3 ne le sont pas non plus.
Ensuite, on peut relier le comportement quadratique de p modulo q à celui de q modulo p :

Théorème 3.1 (Réciprocité quadratique)**.** *Soient p et q premiers impairs, on a* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Ce théorème permet de simplifier le calcul d'un symbole de Legendre.

Exemple 3.2. On a, par exemple, $\left(\frac{-6}{73}\right) = \left(\frac{-1}{73}\right)\left(\frac{2}{73}\right)\left(\frac{3}{73}\right)$. Or $73 \equiv 1[4]$ donc $\left(\frac{-1}{73}\right) = 1$ et $73 \equiv 1[8]$ donc $\left(\frac{2}{73}\right) = 1$. De plus, $\left(\frac{3}{73}\right) = \left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$. Ainsi, -6 est un carré modulo 73.

3.2 Somme de carrés

On s'intéresse à un premier problème : quels sont les entiers qui s'écrivent comme somme de carrés ?

3.2.1 Somme de deux carrés

On définit $\Sigma = \{a^2 + b^2,\ a, b \in \mathbb{N}\}$. On se demande quels nombres entiers appartiennent à cet ensemble. Pour répondre à cette question, on utilise les corps quadratiques et plus précisément l'anneau des entiers de Gauss.
Commençons par remarquer que l'ensemble Σ est stable par multiplication puisque

$$n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[\mathrm{i}],\ n = N(z)(= z\overline{z}).$$

On aura besoin du lemme suivant pour la suite.

Lemme 3.1. *Soit p un nombre premier, alors $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$.*

Démonstration.

- Supposons que $p \in \Sigma$, alors $p = a^2 + b^2$, avec $a, b \in \mathbb{Z}$. On peut le réécrire $p = (a + \mathrm{i}b)(a - \mathrm{i}b)$, or a, b sont non nuls, donc $a + \mathrm{i}b$, $a - \mathrm{i}b$ ne sont pas inversibles. Ainsi, p n'est pas irréductible.
- Si p n'est pas irréductible alors il s'écrit $p = zz'$ avec z, z' non inversibles. On a donc $N(z) \neq 1 \neq N(z')$. Or $p^2 = N(p) = N(z)N(z')$, donc comme p est premier dans $\mathbb{Z}$, nécessairement $p = N(z)$, donc $p \in \Sigma$.

□

On peut, maintenant, énoncer le théorème des deux carrés pour les entiers premiers.

Théorème 3.2. *Soit p un nombre premier, alors $p \in \Sigma$ si et seulement si $p = 2$ ou $p \equiv 1[4]$.*

Démonstration. On sait que $\mathbb{Z}[\mathrm{i}]$ est factoriel donc euclidien, ainsi on a les équivalence suivantes :

$$\begin{aligned} p \text{ n'est pas irréductible dans } \mathbb{Z}[\mathrm{i}] &\Leftrightarrow (p) \text{ n'est pas premier dans } \mathbb{Z}[\mathrm{i}] \\ &\Leftrightarrow \mathbb{Z}[\mathrm{i}]/(p) \text{ n'est pas intègre.} \end{aligned}$$

De plus, on a l'isomorphisme $\mathbb{Z}[\mathrm{i}] \simeq \mathbb{Z}[X]/(X^2 + 1)$, donc on obtient

$$\mathbb{Z}[\mathrm{i}]/(p) \simeq \mathbb{Z}[X]/(X^2 + 1, p) \simeq (\mathbb{Z}[X]/(p))/(\overline{X^2 + 1}) \simeq \mathbb{F}_p[X]/(\overline{X^2 + 1}).$$

Ainsi,

$$\begin{aligned} p \text{ n'est pas irréductible dans } \mathbb{Z}[\mathrm{i}] &\Leftrightarrow X^2+1 \text{ n'est pas irréductible dans } \mathbb{F}_p[X] \\ &\underset{deg(X^2+1)=2}{\Leftrightarrow} X^2+1 \text{ a une racine dans } \mathbb{F}_p[X] \\ &\Leftrightarrow -1 \text{ est un carré dans } \mathbb{F}_p. \end{aligned}$$

Or, on sait que -1 est un carré dans $\mathbb{F}_2$ et, d'après le critère d'Euler, -1 est un carré dans $\mathbb{F}_p$, pour $p \neq 2$ si et seulement si $p \equiv 1[4]$. Ainsi, en appliquant le lemme, le théorème est démontré. □

Théorème 3.3. *Soit $n \in \mathbb{N}$, alors on a équivalence entre :*

- *$n \in \Sigma$,*
- *pour tout nombre premier $p \equiv 3[4]$, $\nu_p(n) \equiv 0[2]$, où $\nu_p(n)$ est la valuation de p dans la décomposition en facteurs premiers de n.*

Démonstration. On va utiliser le théorème précédent.

- Si $n \in \Sigma$, alors $n = a^2 + b^2$, avec $a, b \in \mathbb{Z}$. On note $d = pgcd(a, b)$, alors $n = d^2(A^2 + B^2)$, où $A = \frac{a}{d}$, $B = \frac{b}{d}$, et donc $pgcd(A, B) = 1$. Soit p un diviseur premier impair de $A^2 + B^2$, alors $p \mid (A + \mathrm{i}B)(A - \mathrm{i}B)$. Supposons par l'absurde que p soit irréductible dans $\mathbb{Z}[\mathrm{i}]$, il est alors premier dans $\mathbb{Z}[\mathrm{i}]$ (puisque ce dernier est factoriel). Ainsi, $p \mid A + \mathrm{i}B$ ou $p \mid A - \mathrm{i}B$, mais par passage au conjugué, si p divise l'un, p divise l'autre. Donc p divise les deux, et ainsi par somme et différence, $p \mid 2A$ et $p \mid 2B$. On applique l'application N : $p^2 \mid 4A^2$ et $p \mid 4B^2$ dans $\mathbb{Z}$. Or p est impair donc, d'après le lemme de Gauss, $p \mid A$ et $p \mid B$. Ce qui est absurde, puisque $pgcd(A, B) = 1$. Donc p n'est pas irréductible dans $\mathbb{Z}[\mathrm{i}]$, ainsi d'après le lemme, $p \in \Sigma$ et par suite, d'après le théorème précédent, $p \equiv 1[4]$. Finalement, les nombres premiers congrus à 3 modulo 4 sont "dans" le d^2 et donc de valuation paire.
- Réciproquement, comme lorsque $p \equiv 3[4]$, $\nu_p(n)$ est pair, n s'écrit

$$n = \left(\prod_{p \equiv 3\ [4]} p^{\frac{\nu_p(n)}{2}} \right)^2 \left(\prod_{p \not\equiv 3\ [4]} p^{\nu_p(n)} \right).$$

  Le produit de gauche est un carré parfait donc il appartient à Σ. Dans le produit de droite, chaque nombre premier p est congru à 1 modulo 4 ou égal à 2, donc appartient à Σ, d'après le théorème précédent. On conclut du fait que Σ est stable par multiplication.

□

Exemple 3.3. Décomposons par exemple $N = 260$ en somme de deux carrés. Pour cela, on va utiliser les entiers de Gauss et la multiplicativité de l'application N.
On a $N = 4 \times 5 \times 13 = 2^2(2^2 + 1^2)(3^2 + 2^2) = 2^2[(2 + i)(2 - i)][(3 + 2i)(3 - 2i)] = 2^2[4 + 7i][4 - 7i] = 2^2(4^2 + 7^2) = 8^2 + 14^2$.

3.2.2 Somme de quatre carrés

On cherche à trouver un nombre de carrés tel que tout nombre soit représentable. On va voir que ce nombre est 4 et qu'il optimal.

Lemme 3.2. *Soit p un nombre premier impair. Alors il existe $(x, y) \in \mathbb{Z}^2$ tels que $1 + x^2 + y^2 = 0[p]$.*

Démonstration. Considérons les ensembles $A = \{1 + x^2,\ x \in \{0, \ldots, \frac{p-1}{2}\}\}$ et $B = \{-y^2,\ y \in \{0, \ldots, \frac{p-1}{2}\}\}$. L'idée est de calculer le cardinal de ces deux ensembles pour montrer qu'ils ne sont pas disjoints. Pour l'instant on a $\#A \leq \frac{p+1}{2}$ et $\#B \leq \frac{p+1}{2}$. Cependant, supposons qu'il existe $x, x' \in \{0, \ldots, \frac{p-1}{2}\}$ tels que $1 + x^2 \equiv 1 + x'^2[p]$, alors $x \equiv x'[p]$ ou $x \equiv -x'[p]$. Or $|x - x'| \leq p - 1$,

donc nécessairement $x = x'$. Ainsi $\#A = \dfrac{p+1}{2}$, et de la même manière, $\#B = \dfrac{p+1}{2}$. Cependant $\mathbb{F}_p$ est de cardinal p. Et $\#A + \#B = p + 1 > p$, donc, d'après le principe des tiroirs, A et B ne sont pas disjoints, et donc il existe $(x, y) \in \mathbb{Z}^2$ tels que $1 + x^2 = -y^2[p]$. □

On peut maintenant énoncer le théorème des quatre carrés de Lagrange.

Théorème 3.4. *Tout entier naturel s'écrit comme somme de quatre carrés.*

Démonstration. Voir [1, Section 6.6 p73] □

Essayons de décomposer un entier en somme de quatre carrés.

Exemple 3.4. Décomposons $323 = 17 \times 19$ comme somme de quatre carrés. Pour cela on va utiliser l'anneau des quaternions. On a $17 = 4^2 + 1^2 + 0^2 + 0^2$ et $19 = 4^2 + 1^2 + 1^2 + 1^2$. Ainsi $|4 + \mathrm{i}|^2 = 17$ et $|4 + \mathrm{i} + \mathrm{j} + \mathrm{k}|^2 = 19$. Or $(4 + \mathrm{i})(4 + \mathrm{i} + \mathrm{j} + \mathrm{k}) = 15 + 8\mathrm{i} + 3\mathrm{j} + 5\mathrm{k}$. Donc $323 = 15^2 + 8^2 + 3^2 + 5^2$.

Le nombre optimal de carrés est bien 4, d'après la proposition suivante.

Proposition 3.3. *Aucun nombre de la forme $8n + 7$ ne peut s'exprimer sous la forme de 3 carrés.*

Démonstration. Les carrés modulo 8 sont 0, 1 et 4. En essayant toutes les combinaisons possibles, on voit que $a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5, 6[8]$ donc n'est jamais congru à 7. Les nombres de la forme $8n + 7$ ne peuvent donc pas s'écrire comme somme de 3 carrés. □

4 Représentation par des formes quadratiques

On veut maintenant généraliser le théorème des deux carrés.
Etant donnée une forme quadratique $q(x, y) = ax^2 + bxy + cy^2$, avec $a, b, c \in \mathbb{Z}$, on se demande quels entiers n s'écrivent $n = q(x, y)$, avec $x, y \in \mathbb{Z}$. Dans la suite, on notera (a, b, c) pour la forme quadratique $q(x, y) = ax^2 + bxy + cy^2$.

Définition 4.1. Pour une forme quadratique (a, b, c), on note $\Delta(q) = b^2 - 4ac$ son *discriminant* et $Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ sa matrice.

Remarquons que l'on a $q(x, y) = (x, y)Q\ {}^t(x, y)$ et $\Delta(q) = -4 \det(Q)$.

Définition 4.2.
- On dit que $n \in \mathbb{Z}$ est *repésentable* par la forme (a, b, c), s'il existe $x, y \in \mathbb{Z}$ tels que $n = ax^2 + bxy + cy^2$.
- On dit que $n \in \mathbb{Z}$ est *proprement représentable* par la forme (a, b, c), s'il existe $x, y \in \mathbb{Z}$ premiers entre eux tels que $n = ax^2 + bxy + cy^2$.

Remarque. Ces deux problèmes sont équivalents car n est représenté par q si et seulement si il existe m tel que $m^2 \mid n$ et $\dfrac{n}{m^2}$ est proprement représenté par q.
En effet, si n est représenté par q, $n = q(x, y)$. Si x et y sont premiers entre eux alors $m = 1$ convient et n est proprement représenté par q. Sinon, on note $d = pgcd(x, y)$, on obtient alors $n = d^2 q(\frac{x}{d}, \frac{y}{d})$ et $m = d$ convient. Réciproquement, s'il existe un tel m, $\dfrac{n}{m^2} = q(x, y)$, ainsi $n = q(mx, my)$.

4.1 Formes équivalentes

On commence par définir une relation d'équivalence sur l'ensemble des formes quadratiques. On pourra ensuite s'intéresser aux différentes classes d'équivalence.

Définition 4.3. On dit que deux formes quadratiques q et q' sont *équivalentes* s'il existe $M \in \mathrm{SL}_2(\mathbb{Z})$ tel que $q' \circ M = q$. On note alors $q \sim q'$. Matriciellement, cela s'écrit $Q' = {}^tMQM$.

Remarque. Cela définit une action à droite de $\mathrm{SL}_2(\mathbb{Z})$ sur l'ensemble des formes quadratiques.

Proposition 4.1. *La relation $\sim$ est une relation d'équivalence sur l'ensemble des formes quadratiques.*

De l'écriture matricielle, on déduit :

Proposition 4.2. *Si deux formes sont équivalentes alors elles ont même discriminant.*

Remarque. Remarquons que $\Delta(q) \equiv b^2[2]$, ainsi la parité de b est invariante par action de $\mathrm{SL}_2(\mathbb{Z})$.

Comme les matrices de $\mathrm{SL}_2(\mathbb{Z})$ sont des automorphismes de $\mathbb{Z}^2$, on a le résultat suivant :

Proposition 4.3. *Deux formes équivalentes représentent (proprement) les mêmes entiers.*

Pour résoudre notre problème, il suffit donc de s'intéresser à une seule forme quadratique par classe d'équivalence. On va voir laquelle dans la partie suivante.

4.2 Réduction des formes définies postivies

On veut réduire l'étude de chaque classe d'équivalence à l'étude d'une seule forme quadratique, pour cela on s'intéresse à la réduction des formes quadratiques. On se limitera au cas des formes quadratiques définies positives car les autres cas sont plus compliqués, comme on l'indiquera par la suite.
Rappelons une première définition.

Définition 4.4. On dit que la forme quadratique (a, b, c) est *définie positive* si $\Delta < 0$ et $a > 0$ (donc $c > 0$).

Exemple 4.1. La forme $(1, 0, 1)$ est définie positive.

Définition 4.5. On dit que la forme quadratique (a, b, c) est *réduite* si

$$-a < b \leq a < c \text{ ou } 0 \leq b \leq a = c.$$

Les formes quadratiques réduites sont les formes quadratiques qui nous intéressent :

Théorème 4.1. *Toute forme définie positive est équivalente à une unique forme quadratique réduite.*

Démonstration. La preuve se fait de manière constructive. On part de $q = (a, b, c)$ quelconque. La transformation $(a, b, c) \sim (c, -b, a)$ échange a et c en laissant $|b|$ inchangé. Cela correspond à l'action de $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. On peut donc se ramener à avoir $a \leq c$. La transformation $(a, b, c) \sim (a, b + 2\delta a, c')$ où δ est choisi tel qu'on ait $-a < b' \leq a$ et c' est choisi de manière à conserver le discriminant, permet de diminuer $|b|$ en laissant a inchangé. Cela correspond à l'action de $M_\delta = \begin{pmatrix} 1 & \delta \\ 0 & 1 \end{pmatrix}$. En appliquant alternativement ces deux transformations, on obtient que $(a, b, c) \sim (a_0, b_0, c_0)$, où $-a_0 \leq b_0 \leq a_0 \leq c_0$. Si $b_0 = -a_0$, on applique la transformation $(a_0, b_0, c_0) \sim (a_0, a_0, c_0)$, qui correspond à l'action de $M' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Si $a_0 = c_0$ et $b_0 < 0$ alors l'action de M permet de remplacer b_0 par $-b_0$.
Ainsi toute forme quadratique est équivalente à une forme réduite.
Pour l'unicité, voir [1, Section 6.5.3 p.71]. □

Remarque. Lorsqu'on ne se restreint pas aux formes définies positives, l'unicité n'est plus vérifiée. De plus, vérifier que deux formes réduites sont équivalentes se révèle être assez compliqué.

Réduisons une forme quadratique définie positive à l'aide de l'algorithme donné par la preuve.

Exemple 4.2. Réduisons la forme $(10, 34, 29)$. On a

$$(10, 34, 29) \underset{M_2}{\sim} (10, -6, 1) \underset{M}{\sim} (1, 6, 10) \underset{M_{-3}}{\sim} (1, 0, 1).$$

Pour savoir si une forme quadratique donnée représente un entier, il suffit donc d'étudier sa forme réduite. On pourra, en plus, conclure pour toutes les formes quadratiques de la même classe d'équivalence.

Exemple 4.3. D'après l'exemple précédent, la forme $q = (10, 34, 29)$ est équivalente à $(1, 0, 1)$. On est donc ramené au problème de la somme des deux carrés. Ainsi, pour que n soit représentable par q il faut et il suffit que les nombres premiers congrus à 3 modulo 4, apparaissent avec un exposant pair dans la décomposition en facteurs premiers de n.

On sait maintenant qu'on a une partition de l'ensemble des formes quadratiques définies positives en classes d'équivalence et qu'à chaque classe d'équivalence, on associe une unique forme quadratique réduite. Si on complique un peu notre problème et qu'on cherche à savoir si une forme quadratique de discriminant $\Delta < 0$ donné représente notre entier n, on sait qu'il suffit de regarder les formes réduites de discriminant Δ mais encore faut-il qu'il n'y en ait qu'un nombre fini.
A l'aide du lemme suivant, on peut trouver toutes les formes quadratiques réduites de discriminant donné.

Lemme 4.1. *Si (a, b, c) est définie positive réduite alors $a \leq \frac{\sqrt{|\Delta|}}{\sqrt{3}}$.*

De ce lemme, on déduit le résultat suivant.

Théorème 4.2. *Il n'existe qu'un nombre fini de classes d'équivalence de formes quadratiques définies positives de discriminant $\Delta < 0$ donné. Ce nombre, noté $h(\Delta)$ est appelé nombre de classes.*

Soyons rassurés : notre problème ne demande qu'un nombre fini de vérifications !

4.3 Synthèse

Théorème 4.3. *Soient $n \in \mathbb{Z}$ et $\Delta \in \mathbb{Z}$. Alors il existe une forme quadratique de discriminant Δ qui représente proprement n si et seulement si Δ est un carré modulo $4n$.*

Démonstration. Supposons que $\Delta \equiv k^2[4n]$. Soit m tel que $\Delta = 4nm + k^2$ et soit $q = (n, k, -m)$. Alors q a pour discriminant Δ et elle représente proprement n puisque $q(1, 0) = n$.
Réciproquement, supposons que $n = q(p, r)$, avec $q = (a, b, c)$, $b^2 - 4ac = \Delta$ et $pgcd(p, r) = 1$. D'après le théorème de Bézout, il existe u, v tels que $pu - rv = 1$. Alors avec la transformation $M = \begin{pmatrix} p & v \\ r & u \end{pmatrix}$, $q \sim (a', b', c')$, avec $a' = q(p, r) = n$. D'où, comme q et (a', b', c') ont même discriminant, Δ est un carré modulo $4n$. □

Remarque. On obtient ainsi, une nouvelle preuve du théorème des deux carrés.

Méthode : L'entier n est-il représenté par q ?
- Si Δ n'est pas un carré modulo $4|n|$, alors la réponse est non.
- sinon,
  - ◇ On calcule la forme réduite de q.
  - ◇ On liste les formes quadratiques réduites de discriminant Δ : $q_i = (n, b_i, c_i)$.
  - ◇ On compare les formes réduites de q et q_i.

Résolvons un exemple :

Exemple 4.4. On se demande quelle(s) forme(s) quadratique(s) de discriminant -24 représente(nt) 73.

1. Le discriminant -24 est un carré modulo 4×73 si et seulement si -6 est un carré modulo 73. Or d'après l'Exemple 3.2, c'est le cas. Donc 73 est représentable par une forme quadratique de discriminant -24, d'après le Théorème 4.3.
2. On liste l'ensemble des formes quadratiques réduites de discriminant -24. A l'aide du Lemme 4.1, on a $0 < a \leq \sqrt{8} < 3$. Nous avons donc comme possibilités :
   - Si $a = 1$, comme $|b| \leq 1$,
     — $b = -1$: impossible car $|b| = a$ et $b < 0$.
     — $b = 0$: d'où $c = 6$, ce qui donne la forme $(1, 0, 6)$.
     — $b = 1$: d'où $c = \frac{25}{4} \notin \mathbb{Z}$ impossible.
   - Si $a = 2$, comme $|b| \leq 2$,
     — $b = -2$: impossible car $|b| = a$ et $b < 0$.
     — $b = -1$: d'où $c = \frac{25}{8} \notin \mathbb{Z}$ impossible.
     — $b = 0$: d'où $c = 3$, ce qui donne la forme $(2, 0, 3)$.
     — $b = 1$: d'où $c = \frac{25}{8} \notin \mathbb{Z}$ impossible.
     — $b = 2$: d'où $c = \frac{28}{8} \notin \mathbb{Z}$ impossible.

   Donc les formes réduites de discriminant -24 sont $(1, 0, 6)$ et $(2, 0, 3)$.
3. Etudions ces deux formes. Si 73 était représentable par $(2, 0, 3)$, alors il existerait x, y tels que $73 = 2x^2 + 3y^2$, donc $73 \equiv 2x^2[3]$.
   Or $\left(\frac{73}{3}\right) = \left(\frac{1}{3}\right) = 1$ et $\left(\frac{2x^2}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{x^2}{3}\right) = -\left(\frac{x^2}{3}\right) \in \{0, -1\}$. C'est donc impossible.
   Or on sait que 73 est représentable par une de ces deux formes.

Donc la seule forme quadratique de discriminant -24 qui représente 73 est $(1, 0, 6)$.

5 Questions

↪ *Les équations diophantiennes sont-elles utiles dans d'autres domaines ?*
Elles apparaissent en cryptographie dans le codage de texte par chiffrement affine ou chiffrement RSA.On les retrouve aussi pour calculer les décimales de π et dans le Big Data. A COMPLETER

↪ *Pourquoi avoir choisi cet ordre pour les parties ?*
L'idée est la suivante : Les problèmes diophantiens s'écrivent simplement et parfois se résolvent sans trop de problème comme on peut le voir dans la première partie. On a des résultats d'existence de solutions et des ensembles de solutions dans les cas linéaires. On a donc vu la résolution de quelques problèmes et on se demande si il y a des méthodes pour résoudre les équations diophantiennes générales. C'est le cas, il y a par exemple, la réduction modulaire, la descente infinie ou encore l'utilisation des corps quadratiques. C'est la partie II. Maintenant qu'on a vu ces quelques méthodes, on a envie de s'attaquer à des problèmes plus "costauds" que les problèmes linéaires de la partie I, afin de mettre en application nos méthodes. On monte donc en degré et on s'intéresse aux carrés. C'est la partie III. La partie IV arrive ensuite comme en voyant les formes quadratiques binaires comme une généralisation de la somme de deux carrés.

↪ *Quelles activités peut-on proposer au niveau Terminale ou Licence 1 sur les équations diophantiennes ?*
On peut s'intéresser à la résolution d'équations linéaires à 2 variables, mais aussi au cryptage RSA, puisque cela utilise essentiellement des relation modulo. C'est un exemple assez intéressant puisqu'il est utilisé dans la vie de tous les jours. Le reste est plus compliqué à ce niveau.

↪ *La méthode de la descente infinie ne s'utilise-t-elle que pour montrer qu'il n'existe pas de solution non-triviale ? Comment définit-on l'adjectif "triviale" ?*

C'est Pierre de Fermat qui a trouvé la méthode de la descente infinie et il ne l'utilisait que pour montrer qu'il n'existait pas de solution d'un certain type. En fait, on peut l'utiliser pour montrer qu'une propriété $P(n)$ est fausse pour tout n. Ce n'est pas réduit au cas de l'existence de solution non triviale. Par exemple, on peut montrer à l'aide de la méthode de la descente infinie que $\sqrt{2}$ est irrationnel.

L'adjectif "triviale" caractérise les solutions qu'on voit du premier coup, au sens où soit tous les membres sont nuls, soit au moins un est nul.

↪ *Existe-t-il un algorithme prenant en entrée une équation diophantienne et qui dit si cette équation a une solution ou non ?*

Il n'existe pas d'algorithme universel permettant de décider si une équation diophantienne a une solution en nombre entiers, c'est le théorème de Matiyasevich (1970). Cela répond négativement au dixième problème de Hilbert :

"On donne une équation de Diophante à un nombre quelconque d'inconnues et à coefficients entiers rationnels : on demande de trouver une méthode par laquelle, au moyen d'un nombre fini d'opérations, on pourra distinguer si l'équation est résoluble en nombre entiers rationnels."

↪ *Existe-t-il un théorème des trois carrés ?*

Oui : un entier naturel est somme de trois carrés d'entiers si et seulement si il n'est pas de la forme $4j \times (8k-1)$ avec $j, k \in \mathbb{N}$. La démonstration utilise la loi de la réciprocité quadratique, et l'étude de la classe d'équivalence de la forme quadratique $x_1^2 + x_2^2 + x_3^2$.

↪ *Est-ce que quelqu'un s'est déjà intéressé à la représentation des entiers par une somme de cubes ou même de puissances k-ièmes ?*

Oui, c'est le problème de Warning (1770). On se demande si, pour tout entier naturel k, il existe un nombre $g(k)$ tel que tout entier soit somme de $g(k)$ puissances k-ièmes d'entiers. Hilbert, en 1909, répondit par l'affirmative. Cependant, comme pour le nombre de Frobenius, on ne connait pas de formule explicite pour $g(k)$.

↪ *Résoudre $x^y = y^x$, avec $x, y \in \mathbb{N}^*$.*

Soit (x, y) une solution. Commençons par remarquer que l'ensemble $\{(x, x), x > 0\}$ est solution. Comme x et y jouent des rôles symétriques, supposons maintenant $x < y$. L'équation se réécrit $\dfrac{\ln(x)}{x} = \dfrac{\ln(y)}{y}$. Par étude de la fonction $x \mapsto \dfrac{\ln(x)}{x}$, celle ci est continue et strictement décroissante sur $[e, +\infty]$, donc bijective sur $[e, +\infty]$. Ainsi, si $x > 2$, alors nécessairement $x = y$. Etudions maintenant le cas $x < 3$. Si $x = 1$ alors nécessairement, $y = 1$. Si $x = 2$ alors l'équation s'écrit $2^y = y^2$. L'idée est que par comparaison asymptotique, 2^y tend plus vite vers l'infini que y^2. L'équation se réécrit $y\ln(2) = 2\ln(y)$. Traçons le tableau de variations de la fonction $g : y \mapsto y\ln(2) - 2\ln(y)$:

x	2	$\frac{2}{ln(2)}$	5	$+\infty$
$g'(x)$		$-$ 0	$+$	
$g(x)$	$\searrow$	< 0	$\nearrow > 0 \nearrow$	$+\infty$

Donc pour tout $y \geq 5$, $2^y > y^2$. Ainsi, nécessairement, $y < 5$. On essaye tous les cas possibles, et on obtient $y = 4$. Réciproquement, on vérifie que ce sont bien des solutions. Donc l'ensemble des solutions est $\{(x, x),\ x \in \mathbb{N}^*\} \cup \{(1, 1), (2, 4), (4, 2)\}$.

↪ *Si on modifie un peu une équation diophantienne : résoudre $x^2 + 2y^2 = z^2$.*

Soit (x, y, z) une solution. Comme l'équation est homogène, on peut supposer, quitte à diviser par $pgcd(x, y, z)$ qu'ils sont premiers entre eux dans leur ensemble. On en déduit donc que x, y et z sont premiers entre eux deux à deux. Supposons que x et y soient impairs alors en réduisant modulo 4, $3 \equiv z^2[4]$, ce qui est impossible car les seuls carrés modulo 4 sont 0 et 1. Donc x ou y est pair. Mais, si x est pair alors z est pair, ce qui contredit le fait qu'ils sont premiers entre eux. Donc y est impair, x est pair et z est impair. En raisonnant comme

pour l'équation de Fermat pour $n = 2$, on obtient que $z - x = 2u$ et $z + x = 2v$, où u et v sont premiers entre eux et de parité différente. Lorsqu'on replace dans l'équation, on obtient, $y^2 = 2uv$. Comme u et v sont de parité différentes, l'un des deux est pair. Disons $u = 2a$, c'est à dire $y^2 = 4av$ et donc en regardant la décomposition en facteurs premiers, on obtient que $a = r^2$ et $v = s^2$ avec r et s premiers entre eux. On obtient alors $y = 2rs$, $z = s^2 + 2r^2$ et $x = s^2 - 2r^2$, avec r et s premiers entre eux. On vérifie que c'est bien une solution de l'équation. On a donc obtenu l'ensemble des solutions.

↪ *Peut-on trouver quatre nombres premiers entre eux dans leur ensemble et tels que dès qu'on en enlève un, ils ne sont plus premiers dans leur ensemble ?*
On considère les quatre premiers nombres premiers 2, 3, 5, 7. On prend $x = 2 \times 3 \times 5$, $y = 3 \times 5 \times 7$, $z = 2 \times 5 \times 7$, $t = 2 \times 3 \times 7$. Alors ces quatre nombres répondent à la question.
Remarque. On utilise cette méthode dans la démonstration de la décomposition de Dunford.

Références

[1] DUVERNEY. D, 2007. *Théorie des nombres*. Dunod.

[2] DE KONINCK. J-M, MERCIER. A, 2004. *1001 problèmes en théorie classique des nombres*. Ellipses.

[3] COMBES. F, 1998. *Algèbre et géométrie*. Bréal.

[4] FRANCINOU. S, GIANELLA. H, NICOLAS.S, 2009 *Exercices de mathématiques. Oraux X-ENS. Analyse 2*. Cassini.

[5] PERRIN.D, 1996 *Cours d'algèbre*. Ellipses.

[6] BERHUY.G, 2012 *Modules : théorie, pratique... et un peu d'arithmétique*. Calvage et Mounet.