L'équation de Pell-Fermat

Gabrielle Lalou, Daniel Berda

Table des matières

Introduction

Cet exposé est dédié à l'équation de Pell-Fermat. Il s'agit de l'équation $x^2 - dy^2 = 1$ où $d \in \mathbb{Z}$ est un paramètre fixé et dont les solutions sont les couples d'entiers $(x, y) \in \mathbb{Z}^2$. L'ensemble des solutions (sous forme de couples) sera noté $S_d = \{(x, y) \mid x^2 - dy^2 = 1\}$.
L'un des résultats les plus connus qui concerne cette équation est sans doute le fait que ses solutions sont régies par une structure de groupe. Nous souhaitons dans cet exposé développer ce point et caractériser précisément cette structure de groupe. À cette fin, nous serons amenés à étudier les réels de la forme $z+y\sqrt{d}$ obéissant à une structure algébrique familière et à partir desquels nous pourrons construire un groupe isomorphe à S_d.$L'ensemble\{x+y\sqrt{d} \mid (x, y) \in \mathbb{Z}^2\}$ sera noté $\mathbb{Z}[\sqrt{d}]$.
En outre, nous serons peut-être également amenés à définir une norme sur ces réels. Aussi avons-nous jugé opportun d'introduire dès maintenant la notation peu standard suivante : $N_1(d)$ pour désigner l'ensemble des éléments de norme 1. $N_1(d) = \{z \in \mathbb{Z}[\sqrt{d}] \mid N(z) = 1\}$

Dans cet exposé, nous nous limiterons à cette approche algébrique et ne présenterons pas de résolution à proprement dite de l'équation de Pell-Fermat. Cela nécessiterait par exemple d'employer la méthode des fractions continues pour déterminer une solution particulière (comme la solution minimale présentée en fin d'exposé).

Chapitre 1

L'équation de Pell-Fermat : son histoire, premières solutions

1.1 Éléments historiques

1.1.1 L'équation de Pell-Fermat dans l'antiquité

On retrouve des traces de cette équation qui remontent à l'antiquité avec le problème des boeufs d'Hélios attribué à Archimède. Il est question de déterminer le nombre d'animaux dans un troupeaux en imposant des conditions arithmétiques liées à la couleur de leur robe, ce qui amène à la résolution de l'équation $x^2 - 410286423278424y^2 = 1$. Si une première solution a été obtenue en 1880 par Carl Ernst August Amthor, il a fallu attendre 1965 pour obtenir une expression explicite de la solution minimale avec le développement des outils informatiques. Un apport majeur nous est dû à Diophante d'Alexandrie (214- 298 ca.) dans ses *Arithmétiques* qui y expose une paramétrisation explicite des solutions rationnelles.

1.1.2 Avancée indienne :

Les travaux de Diophante ont été suivi d'un silence de près de deux siècles avant l'arrivée des mathématiciens et astronomes indiens Aryabhata (476-550) et Bramagupta (598-668).
Une identité fondamentale porte désormais le nom de Brahmagupta.

Identité de Bramagupta : Soient $x, y, z, t, d \in \mathbb{Z}$, on a :

$$\left(x^2 - dy^2\right)\left(z^2 - dt^2\right) = (xz + dyt)^2 - d(xt + yz)^2$$

La vérification de cette identité est immédiate en développant les produits.

Théorème : Une solution en appelle une autre.
Pour $d \in \mathbb{Z}$, l'application qui à deux couples d'entiers (x, y) et (z, t), associe le couple $(zx + dyt, xt + yz)$ induit une structure de groupe abélien sur l'ensemble des solutions de l'équation de Pell-Fermat S_d.

Preuve : Remarquons que si $(x, y), (z, t) \in S_d$, alors l'identité de Brahmagupta nous fournit la solution $(zx + dyt, xt + yz)$.
On a ainsi défini une loi de composition interne sur l'ensemble S_d des solutions de l'équation notée $\cdot$.
Vérifions l'associativité : Soient $(x, y), (z, t)$ et $(u, v) \in S$.

$$\begin{aligned}((x, y) \cdot (z, t)) \cdot (u, v) &= (zx + dyt, xt + yz) \cdot (u, v) \\ &= (u(zx + dyt) + dv(xt + yz), v(zx + dyt) + u(xt + yz)) \\ &= (x, y) \cdot ((z, t) \cdot (u, v))\end{aligned}$$

Et on vérifie la commutativité :

$$\begin{aligned}(x, y) \cdot (z, t) &= (zx + dyt, xt + yz) \\ (z, t) \cdot (x, y) &= (zx + dty, zy + tx)\end{aligned}$$

et ces deux quantités sont égales.
L'élément neutre pour cette loi de groupe est le couple $(1, 0)$ et l'inverse de $(x, y) \in S_d$ est $(x, -y)$.

Les techniques introduites par Aryabhata et Brahmagupta sont par la suite reprises et améliorées par des mathématiciens dont Bhaskara II (1114-1185) qui a élaboré la méthode chakravala combinant l'identité de Brahmagupta et le théorème des restes chinois. Elle repose sur un fonctionnement similaire à la méthode des fractions continues évoquée en introduction.

1.1.3 Le défi de Fermat

En 1657 après une longue période silencieuse, l'équation de Pell-Fermat refait surface en Europe à travers un défi lancé par le mathématicien français Pierre de Fermat (1601-1665) à Bernard Frénicle de Bessy (1600 ca.-1674). Dans ce problème il était question de déterminer les solutions entières de l'équation $x^2 - 61y^2 = 1$. La plus petite solution non triviale correspond au couple (1766319049, 226153980). Il faudra attendre les travaux de Joseph-Louis Lagrange (1736-1813) qui fournit une preuve rigoureuse de l'existence d'une infinité de solutions basée sur les fractions continues de Léonard Euler (1707-1783). Léonard Euler ayant introduit les fractions continues à la suite de la solution proposée par William Brounker (1620-1684) au problème de Fermat, elle-même similaire à la méthode indienne chakravala. Notons que le nom de Pell qui a été retenu pour cette équation provient d'une erreur de Léonard Euler lui ayant attribué par erreur le crédit de la solution qui avait été en fait proposée par Brounker.

1.2 Premières solutions

On rappelle que nous nous intéressons aux solutions $(x, y) \in \mathbb{Z}^2$ de l'équation $x^2 - dy^2 = 1$ où $d \in \mathbb{Z}$ est un paramètre fixé. Nous pouvons déjà fournir les solutions de cette équations pour certaines valeurs de d.
On remarque que quelque soit d, l'équation possède les solutions $(\pm 1, 0)$. Nous les appellerons les **solutions triviales**.
Si d = 0, nous obtenons les solutions $(\pm 1, y)$ pour tout $y \in \mathbb{Z}$.
Si d = -1, nous obtenons les solutions supplémentaires $(0, \pm 1)$.
Ainsi, si $d < -1$, l'équation ne possède que des solutions triviales . En effet, pour toute solution (x, y) non triviale, $y \neq 0$ donc $|y| >= 1$ ce qui entraine immédiatement $1 = x^2 - dy^2 = x^2 + |d|y^2 \geq |d|$. Comme $d < 0$, ceci entraîne que $d = -1$.
Enfin, si $d = -1$, il s'agit de résoudre $x^2 + y^2 = 1$ dont les solutions sont $(\pm 1, 0)$ et $(0, \pm 1)$.
Il nous reste un dernier cas facile à résoudre. Il s'agit du cas où d est le carré d'un entier, ce qui nous amène à résoudre $x^2 - (ny)^2 = 1$ soit $(n - ny)(n + ny) = 1$, ce qui entraîne $x - ny = \pm 1$ et $x + ny = \pm 1$. La résolution de ces deux systèmes simples nous donne systématiquement un couple (x, y) où $y = 0$, c'est-à-dire une solution triviale.
Par cette étude, nous pouvons désormais nous limiter au cas où $d > 0$ n'est pas un carré. Nous maintiendrons cette hypothèse dans tout ce qui va suivre.

Chapitre 2

De l'anneau $\mathbb{Z}[\sqrt{d}]$ aux solutions de l'équation de Pell-Fermat

2.1 Premières définitions

2.1.1 Définitions : Anneau, Sous-anneau

Un **anneau (unitaire)** $(A, +, \cdot)$ est un ensemble A munit de deux lois de compositions interne :

— l'addition notée $+ : A \times A \to A, (a, b) \mapsto a + b$

— la multiplication notée $\cdot$: A$\times A \to A, (a, b) \mapsto a \cdot b$

qui satisfont les propriétés suivantes :

1. $(A, +)$ est un groupe commutatif dont on note 0_A sont élément neutre et $-a$ l'opposé de a pour tout a dans A.
2. la loi $\cdot$ est associative.
3. $\cdot$ est distributive par rapport à $+$.
4. $(A, \cdot)$ a un élément neutre noté 1_A.

Un **sous-anneau** de $(A, +, \cdot)$ est un sous-ensemble B de A, stable pour les deux opérations de A avec la propriété que B, muni de la restriction de ces deux opérations, soit un anneau et que $1_A = 1_B$.

2.1.2 $(\mathbb{Z}[\sqrt{d}], +, \times)$ comme sous-anneau de $\mathbb{R}$

Il s'agit de vérifier que $\mathbb{Z}[\sqrt{d}]$ vérifie la définition d'un sous-anneau. Nous rappelons que l'anneau $\mathbb{R}$ est muni de l'addition et du produit standard.
Soient $x + y\sqrt{d}$ et $x' + y'\sqrt{d}$ deux éléments de $\mathbb{Z}[\sqrt{d}]$

- L'élément neutre de $\mathbb{R}$ est 0, qui correspond à $0 = 0 + 0\sqrt{d}$, qui est donc bien dans $\mathbb{Z}[\sqrt{d}]$.

- $x + y\sqrt{d} + x' + y'\sqrt{d} = (x + x') + (y + y')\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ donc $\mathbb{Z}[\sqrt{d}]$ est stable par l'addition standard.
- Nous vérifions également la stabilité par la multiplication standard. $(x + y\sqrt{d})(x' + y'\sqrt{d}) = (xx' + yy'd) + (xy' + x'y)\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$

Comme $\mathbb{R}$ est intègre, ce résultat entraîne immédiatement que $\mathbb{Z}[\sqrt{d}]$ est intègre.

2.2 $\mathbb{Z}[\sqrt{d}]$ et écriture unique

Dans cette section, nous souhaitons montrer que tout élément de $\mathbb{Z}[\sqrt{d}]$ peut être identifié par un unique couple $(a, b) \in \mathbb{Z}^2$

Preuve : Par l'absurde, on suppose qu'il existe $\alpha \in \mathbb{Z}[\sqrt{d}]$ et $(x, y), (a, b) \in \mathbb{Z}^2$ deux couples d'entiers distincts tels que

$$\alpha = x + y\sqrt{d} = a + b\sqrt{d}$$

On a alors l'inégalité suivante :

$$\begin{aligned} & x - a + (y - b)\sqrt{d} = 0 \\ \Leftrightarrow & \sqrt{d} = \frac{a - x}{y - b} \\ \Leftrightarrow & \sqrt{d} \in \mathbb{Q} \end{aligned}$$

d étant supposé non carré, nous déduisons que $\sqrt{d} \in \mathbb{Q}$ est absurde.
On en déduit finalement

$$\forall \alpha \in \mathbb{Z}[\sqrt{d}] \ , \ \exists!(a, b) \in \mathbb{Z}^2 \ , \ \alpha = a + b\sqrt{d}$$

.

2.3 Conjugaison dans $\mathbf{Z}[\sqrt{d}]$

Nous allons maintenant définir un équivalent à la conjugaison complexe dans notre anneau. Cette notion deviendra bientôt indispensable dans notre étude. Rappelons avant cela la définition suivante.

Définition : Un automorphisme d'anneaux est un morphisme bijectif de l'anneau vers lui-meme.
En particulier, l'application

$$\sigma : \begin{cases} \mathbb{Z}[\sqrt{d}] \to \mathbb{Z}[\sqrt{d}] \\ x + y\sqrt{d} \mapsto x - y\sqrt{d} \end{cases}$$

est un automorphisme d'anneaux.

Preuve : Nous commençons par montrer que σ est un **morphisme :**
On a

$$\sigma(1) = 1$$

et

$$\forall x, y \in \mathbb{Z}[\sqrt{d}],\ \exists!(a,b) \in \mathbb{Z}^2,\ \exists!\,(a',b') \in \mathbb{Z}^2,\ \begin{cases} x = a + b\sqrt{d} \\ y = a' + b'\sqrt{d} \end{cases}$$

d'où :

$$\begin{aligned} \sigma(x+y) &= \sigma\left(a + a' + \sqrt{d}\,(b+b')\right) \\ &= (a - b\sqrt{d}) + \left(a' - b'\sqrt{d}\right) \\ &= \sigma(x) + \sigma(y) \end{aligned}$$

puis

$$\begin{aligned} \sigma(xy) &= \sigma\left(aa' + bb'd + \sqrt{d}\,(a'b + ba)\right) \\ &= aa' + bb'd - \sqrt{d}\,(a'b + b'a) \\ &= (a - b\sqrt{d})\left(a' - b'\sqrt{d}\right) \\ &= \sigma(x)\sigma(y) \end{aligned}$$

De plus, σ est une **bijection** car $\sigma \circ \sigma(x) = x$.
On a donc montré que σ est un automorphisme d'anneau de $\mathbb{Z}[\sqrt{d}]$.

2.4 Norme sur $\mathbb{Z}[\sqrt{d}]$:

Analogue au module complexe, nous définissons sur $\mathbb{Z}[\sqrt{d}]$ une norme comme suit.

Définition : La norme est l'application

$$N : \begin{cases} \mathbb{Z}[\sqrt{d}] \to \mathbb{Z} \\ \alpha = x + y\sqrt{d} \mapsto \alpha\sigma(\alpha) = x^2 - dy^2 \end{cases}$$

Nous insistons sur le fait que la norme renvoie un élément de $\mathbb{Z}[\sqrt{d}]$ sur $\mathbb{Z}$.

Propriétés de N : Elle vérifie les trois points suivants :
1. $N(\alpha) = 0 \Leftrightarrow \alpha = 0$,
2. $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{d}],\ N(\alpha\beta) = N(\alpha)N(\beta)$,
3. $\alpha \in \mathbb{Z}[\sqrt{d}]$ inversible $\Leftrightarrow N(\alpha) = \pm 1$.

Preuve : Nous commençons par rappeler qu'en tant que sous anneau de l'anneau intègre $\mathbb{R}$, l'anneau $\mathbb{Z}[\sqrt{d}]$ est intègre.

1. Ainsi : $N(\alpha) = \alpha\sigma(\alpha) = 0 \Leftrightarrow \alpha = 0$ ou $\sigma(\alpha) = 0$.
Et comme σ est injective (car bijective), on a $\sigma(\alpha) = 0 \Rightarrow \alpha = 0$.

2. Comme σ est un morphisme d'anneaux, on a $N(\alpha\beta) = \alpha\beta\sigma(\alpha\beta) = \alpha\sigma(\alpha)\beta\sigma(\beta) = N(\alpha)N(\beta)$.

3. On pose $\{\pm 1\}$ le groupe des inversibles pour la multiplication de $\mathbb{Z}$.
($\Rightarrow$) α est inversible d'inverse β, alors on $a : 1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta)$ donc $N(\alpha)$ est inversible dans $\mathbb{Z}$, d'où $N(\alpha) = \pm 1$ (car $N(\alpha) \in \mathbb{Z}$).
($\Leftarrow$)Réciproquement, si $N(\alpha) \in \{\pm 1\}$, alors on peut poser $y = \frac{\sigma(\alpha)}{N(\alpha)} = \pm\sigma(\alpha) \in \mathbb{Z}[\sqrt{d}]$ tel que $\alpha y = \frac{N(\alpha)}{\sigma(\alpha)}\frac{\sigma(\alpha)}{N(\alpha)} = 1$ donc α est inversible d'inverse y.

2.5 Vers les solutions de l'équation de Pell-Fermat

Nous rappellons qu'à chaque anneau $(A, +, \cdot)$ nous pouvons considérer un groupe $(A^\times, \cdot)$ appelé le groupe unité de A constitué de l'ensemble des éléments inversibles de A pour la loi multiplicative.
Exemple : $\mathbb{Z}^\times = \{\pm 1\}$ est un groupe pour la multiplication usuelle.
Nous avons vu précédemment que $N(\mathbb{Z}[\sqrt{d}]^\times) = \{\pm 1\}$
et que $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{d}], N(\alpha\beta) = N(\alpha)N(\beta)$. Ceci montre que l'application
$N : \mathbb{Z}[\sqrt{d}]^\times \to \mathbb{Z}^\times$ est un homomorphisme de groupes.
Par conséquent, son noyau noté $N_1(d) = \{z \in \mathbb{Z}[\sqrt{d}]^\times N(z) = 1\}$ est un groupe.
Soit

$$f : \begin{cases} \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}[\sqrt{d}] \\ (x, y) \mapsto x + y\sqrt{d} \end{cases}$$

L'écriture unique de tout élément de $\mathbb{Z}[\sqrt{d}]$ comme un couple d'entiers se traduit ici par la bijectivité de f.
Nous pouvons de plus montrer que Im $f_{|S} = N_1(d)$ en notant $N_1(d)$ **les éléments de $\mathbb{Z}[\sqrt{d}]$ de norme 1**.
En effet, $\forall (x, y) \in S$, $N(f(x, y)) = 1$ ce qui montre que $Imf_{|S} \subset N_1(d)$.
Réciproquement, si $z \in N_1(d)$, $N(z) = 1$ et on écrit $z = a + b\sqrt{d} = a^2 - db^2 = 1$,
donc $f(a, b) = z$ et $(a, b) \in S$ et on a l'inclusion réciproque $N_1(d) \subset Imf|_S$.
Donc comme restriction d'une application bijective,

$$f_{|S} : \begin{cases} S \to N_1(d) \\ (x, y) \mapsto x + y\sqrt{d} \end{cases}$$

est bijective.
D'autre part, nous pouvons montrer que c'est un morphisme de groupe :
Si on note $\cdot$ la loi de groupe sur S : $((x, y) \cdot (z, t)) \mapsto (zx + dyt, xt + yz)$, alors

on a

$$\begin{aligned} f_{|S}((x,y)\cdot(z,t)) &= f_{|S}(zx+dyt, xt+yz) \\ &= (xz+dyt)+(xt+yz)\sqrt{d} \\ &= f_{|S}(x,y)_{|S}(z,t) \end{aligned}$$

et $f_{|S}$ est donc un **isomorphisme de groupes**.

Chapitre 3

Existence d'une solution non triviale

Introduction

Nous avons précédemment établi que l'équation de Pell-Fermat admet des solutions triviales $(\pm 1, 0)$. Une question se pose naturellement : dans le cas encore non résolu où $d > 0$ n'est pas un carré, l'équation admet-elle des solutions non triviales ? C'est ce que nous tâcherons de démontrer dans cette partie.

3.1 Le théorème de Dirichlet

Nous commençons ce chapitre par la proposition suivante qui sera immédiatement appliquée pour démontrer le corollaire du théorème de Dirichlet dont nous avons besoin pour la preuve finale.

Proposition : Pour tout irrationnel $\alpha \in \mathbb{R}$, il existe une infinité de rationnels $x = \frac{p}{q}$ tels que $|\alpha - x| < \frac{1}{q^2}$.

Preuve : On fixe $n > 0$ un entier naturel non nul. On considère l'ensemble $A = \{0, \ldots, n\}$. Comme α est irrationnel, l'application

$$f : \begin{cases} A \to \mathbb{R} \\ a \mapsto \{a\alpha\} \end{cases} \text{ est injective.}$$

En effet, si $f(a) = f(b)$ pour $a, b \in A$, alors on a :

$$\begin{aligned} (a-b)\alpha &= a\alpha - b\alpha \\ &= \{a\alpha\} + \lfloor a\alpha \rfloor - \{b\alpha\} - \lfloor bx \rfloor \\ &= \lfloor a\alpha \rfloor - \lfloor b\alpha \rfloor \in \mathbb{Z} \end{aligned}$$

Si $a \neq b$, $\alpha = \frac{\lfloor a\alpha \rfloor - \lfloor b\alpha \rfloor}{a-b} \in \mathbb{Q}$, ce qui contredit son irrationalité.
On a montré que $a = b$ et donc f est injective.

Par définition de la partie fractionnaire, on a $Imf \subset I = [0,1[$ et on a de plus la disjonction suivante.

$$[0,1[= \bigsqcup_{k=0}^{n-1} \left[\tfrac{k}{n}, \tfrac{k+1}{n}\right[$$

I est une union disjointe de n intervalles, et $|A| = n+1$. Comme f est injective, $|f(A)| = |A| = n+1$. Il y a donc n+1 images à répartir dans une union disjointe de n intervalles, ce qui assure par le principe des tiroirs que deux éléments $a \neq b$ sont envoyés sur le même intervalle de la forme $I_k = [\frac{k}{n}, \frac{k+1}{n}[$.

On peut supposer sans perte de généralité que $a > b$ et on a, comme chaque intervalle I_k est de taille $\frac{1}{n}$, que $|f(a) - f(b)| < \frac{1}{n}$ soit $|\{a\alpha\} - \{b\alpha\}| < \frac{1}{n}$.
Or on a $\{a\alpha\} = a\alpha - \lfloor a\alpha \rfloor$ et $\{b\alpha\} = b\alpha - \lfloor b\alpha \rfloor$.
On peut ainsi réécrire l'inégalité $|q\alpha - p| < \frac{1}{n}$ en posant :

$$\begin{aligned} p &= \lfloor a\alpha \rfloor - \lfloor b\alpha \rfloor \\ q &= a - b \end{aligned}$$

En divisant par $q > 0$, on a :

$$|\alpha - \tfrac{p}{q}| < \tfrac{1}{n|q|}.$$

Et puisque $a - b = q$, où $a, b \in \{0, \ldots, n\}$, on a $q \leq n$, d'où :

$$|\alpha - \tfrac{p}{q}| \leq \tfrac{1}{q^2}.$$

Il nous reste à montrer qu'il existe une infinité de tels rationnels.
Le raisonnement ci-dessus étant valable pour tout entier $n > 0$, posons $x_n = \frac{p}{q}$.
Pour chaque entier $n > 0$, $|\alpha - x_n| < \frac{1}{n|q|} \leq \frac{1}{n}$ car $|q| \geq 1$ puisque $q \neq 0$.
On en déduit en particulier que $x_n \longrightarrow \alpha$.
Montrons que $\{x_n \mid n \in \mathbb{N}\}$ est infini.
Soit $B = \{x_n \mid n \in \mathbb{N}\}$ qu'on suppose par l'absurde fini.
On suppose par l'absurde que $\forall n \in \mathbb{N}$, $x_n \neq \alpha$ alors $\forall n \in \mathbb{N}$, $|x_n - \alpha| > 0$.
Comme B est fini, on peut considérer $m = \min_{n \in \mathbb{N}} |\alpha - x_n|$.
Par définition de la convergence de (x_n), on a :

$$\exists N \in \mathbb{N}, \forall n \geq N, |x_n - \alpha| < \tfrac{m}{2} < m$$

puisque $m > 0$, ce qui contredit la minimalité de m puisque par définition de m, $\forall n \in \mathbb{N}\, |x_n - \alpha| \geq m$.
On en déduit que $\alpha \in B$, ce qui se traduit par :

$$\exists n \in \mathbb{N}, \alpha = x_n \in \mathbb{Q}$$

ce qui contredit immédiatement l'irrationalité de α. On conclut finalement que B est infini.

Remarque : On peut en fait supposer que les entiers p et q de l'énoncé sont premiers entre eux. En effet, si ce n'est pas le cas, notons $p' = \frac{p}{pgcd(p,q)}$ et $q' = \frac{q}{pgcd(p,q)}$.
Alors $q'pgcd(p,q) = q$ donc $q'|q$, d'où $|q'| \leq |q|$, ce qui nous permet d'écrire, en partant de l'inégalité déjà prouvée : $|\alpha - x| \leq \frac{1}{q^2} \leq \frac{1}{q'^2}$.

3.2 Un lemme important qui découle du théorème de Dirichlet

Nous souhaitons démontrer la proposition suivante qui est une application du lemme de Dirichlet qui s'avérera très utile dans notre problème.

Corollaire : Il existe une infinité d'éléments $\alpha \in \mathbb{Z}[\sqrt{d}]$ tels que

$$\begin{cases} \alpha > 2\sqrt{d} - 1 \\ \text{ et} \\ |N(\alpha)| < 2\sqrt{d} + 1 \end{cases}$$

.

Preuve : D'après le théorème de Dirichlet, pour tout $\alpha \in \mathbb{Z}[\sqrt{d}] \subseteq \mathbb{R}$, il existe une infinité de rationels $x = \frac{p}{q} \in \mathbb{Q}$, où $p, q \in \mathbb{Z}$ tels que $|\alpha - x| < \frac{1}{q^2}$.
On remarque qu'en posant $\alpha = \sqrt{d}$, on a $|q\sqrt{d} - p| < \frac{1}{|q|}$.
On suppose que p et q sont premiers entre eux , avec $q > 0$ (ce qui ne change rien d'après la remarque précédente), d'où en procédant étape par étape :
(1) $|q\sqrt{d} - p| < \frac{1}{q} \Leftrightarrow -\frac{1}{q} < q\sqrt{d} - p < \frac{1}{q} \Leftrightarrow q\sqrt{d} - \frac{1}{q} < p < q\sqrt{d} + \frac{1}{q}$
(2) On sait que $\sqrt{d} > 1$, et $q \geq 1$ (car $q \in \mathbb{Z}^*$ par hypothèse), d'où

$$p > q\sqrt{d} - \frac{1}{q} = q\left(\sqrt{d} - \frac{1}{q^2}\right) \geq q(\sqrt{d} - 1) \geq 0.$$

(3) On a alors $p, q > 0$, d'où $|p+q\sqrt{d}| = p+q\sqrt{d}$ et on pose $\alpha = p+q\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

$$2\sqrt{d} - 1 \leq 2q\sqrt{d} - q = q(\sqrt{q} - 1) + q\sqrt{d} < p + q\sqrt{d} = \alpha$$

et

$$\alpha = p + q\sqrt{d} < 2q\sqrt{d} + \frac{1}{q} \leq 2q\sqrt{d} + 1 \leq 2q\sqrt{d} + q.$$

(4)

$$|N(\alpha)| = |\alpha\sigma(\alpha)| = |p + q\sqrt{d}||p - q\sqrt{d}| < (2q\sqrt{d} + q)\frac{1}{q} = 2\sqrt{d} + 1$$

Ces inégalités étant vraies pour tout $\alpha = p + q\sqrt{d}$ où $p \wedge q = 1$, avec α ayant une écriture unique. Ainsi nous avons montré que deux rationnels distincts définissent des éléments distincts de $\mathbb{Z}[\sqrt{d}]$, ce qui conclut la preuve.

3.3 Rappels sur les idéaux et une propriété des anneaux intègres :

Défintions :

- Un sous-ensemble I de A est un idéal de A si :
  — $(\mathrm{I}, +)$ est un sous groupe $(\mathrm{A}, +)$,
  — $\forall a \in \mathrm{A}, \forall b \in I, ab, ba \in I$ (propriété d'absorption).
- Deux éléments a et b d'un anneau A sont associés si : $\exists u \in A^\times, b = ua$ où $A^\times$ est le groupe inversible de A.

On pose : $\forall a \in \mathrm{A}, (a) = \{ab \mid b \in \mathrm{A}\}$ l'idéal de A engendré par a.
On remarque que : $(a) \subseteq (b) \Leftrightarrow b|a \Leftrightarrow \exists c \in \mathbb{Z}, a = bc$.

Lemme : Deux éléments d'un anneau intègre sont associés si, et seulement si ils engendrent le meme idéal.

Preuve : ($\Rightarrow$) Soient a et b deux eléments d'un anneau intègre A.
Si a ou b est nul l'assertion est immédiate, on les suppose donc non nuls.
Si a et b sont associés, alors $\exists u \in A^\times, a = ub$. On a $ub = a \in \{cb \mid c \in A\} = (b)$, ce qui implique que $(a) \subseteq (b)$. Mais par définiton de $A^\times$: $\exists v \in A, uv = vu = 1_A$.
D'où le fait que $b = va$, et donc que $b \in (a)$, ce qui implique que $(b) \subseteq (a)$.
Ainsi $(a) = (b)$ et ils engendrent le même idéal.
($\Leftarrow$) Réciproquement :

$$(a) = (b) \quad \Rightarrow \exists u, v \in A, \begin{cases} b = va \\ a = vb \end{cases} \Rightarrow \exists u, v \in A, \begin{cases} b \in (a) \\ a \in (b) \end{cases} .$$

D'où le fait que $a = vb = vua$ équivaut à $a(1 - vu) = 0$.
Par intégrité de A, et avec $a \neq 0$, on a : $1 - vu = 0 \Rightarrow vu = 1 \Rightarrow u, v \in A^\times$, et a at b sont alors associés.

On rappelle que $(n) = n\mathbb{Z}[\sqrt{d}]$ est l'idéal de $\mathbb{Z}[\sqrt{d}]$ engendré par n.
et la relation suivante définit une relation d'équivalence :
$\forall z, z' \in \mathbb{Z}[\sqrt{d}]$, $z \sim z' \Leftrightarrow z - z' \in I$.

Propositions :

- R est une relation d'équivalence.
  On note $\mathbb{Z}[\sqrt{d}]/(n)$ l'anneau quotient de $\mathbb{Z}[\sqrt{d}]$ par la relation d'équivalence R.
  ie. : $\mathbb{Z}[\sqrt{d}]/(n) := \mathbb{Z}[\sqrt{d}]/R$.
- $\mathbb{Z}[\sqrt{d}]/(n)$ devient un anneau quand on le munit des lois de composition suivantes.

$$+ : \begin{cases} \mathbb{Z}/[\sqrt{a}]/(n) \times \mathbb{Z}[\sqrt{a}]/(n) \to \mathbb{Z}[\sqrt{d}]/(n) \\ ([a],[b]) \mapsto [a+b] \end{cases} \quad \text{d'élément neutre } [0],$$

et

$$\times : \begin{cases} \mathbb{Z}/[\sqrt{a}]/(n) \times \mathbb{Z}[\sqrt{a}]/(n) \to \mathbb{Z}[\sqrt{d}]/(n) \\ ([a],[b]) \mapsto [ab] \end{cases} \quad \text{d'élément neutre } [1].$$

3.4 Le lemme de cardinalité

Lemme : Pour tout entier non nul n, l'anneau quotient $\mathbb{Z}[\sqrt{d}]/(n)$ est fini de cardinal $|\mathbb{Z}[\sqrt{d}]/(n)| = n^2$.

Preuve : On procède étape par étape.
(1) On montre que $\mathbb{Z}^2 \cong Z[\sqrt{d}]$.
La fonction $f : \begin{cases} \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{d}] \\ (x,y) \mapsto x + y\sqrt{d} \end{cases}$ est un isomorphisme de groupes car nous avons prouvé précédemment qu'à tout élément $\alpha \in \mathbb{Z}[\sqrt{d}]$, nous pouvons associer un unique couple (x,y) tel que $\alpha = x + y\sqrt{d}$.
D'où le fait que $\mathbb{Z}^2 \cong Z[\sqrt{d}]$.
(2) On montre que $(n) \cong (n\mathbb{Z})^2$.
Si $\alpha = x + y\sqrt{d} \in (n) = \{nz \mid z \in \mathbb{Z}[\sqrt{d}]\}$, alors on peut écrire

$$\exists (u,v) \in \mathbb{Z}^2,\ \alpha = n(u + v\sqrt{d}) \in (n)$$

On en déduit l'identité : $f^{-1}((n)) = n\mathbb{Z} \times n\mathbb{Z}$.
f étant bijective, on a $(n) \cong (n\mathbb{Z})^2$.
(3) On conclut à l'aide d'un théorème.
On pose π un morphisme surjectif d'anneaux tel que :

$$\pi : \begin{cases} \mathbb{Z}^2 \to (\mathbb{Z}/n\mathbb{Z})^2 \\ (x,y) \mapsto ([x],[y]) \end{cases} \quad \text{où} \quad [t] = t\,(mod\ n).$$

On a

$$\begin{aligned} ker(\pi) &= \{(x,y) \in \mathbb{Z}^2 \mid ([x],[y]) = (0,0)\} \\ &= \{(x,y) \in \mathbb{Z}^2 \mid n|x \text{ et } n|y\} \\ &= (n\mathbb{Z})^2 \end{aligned}$$

Soit $h : G \to H$ un morphisme de groupes, alors $G/\ker(h) \cong \mathrm{Im}(h)$.
On adapte ce théorème à π tel que $\mathbb{Z}^2/(n\mathbb{Z})^2 \cong (\mathbb{Z}/n\mathbb{Z})^2$ avec

$$\left|(\mathbb{Z}/n\mathbb{Z})^2\right| = |(\mathbb{Z}/n\mathbb{Z})|^2 = n^2$$

On en déduit que $\mathbb{Z}[\sqrt{d}]/(n) \cong \mathbb{Z}^2/(n\mathbb{Z})^2 \cong (\mathbb{Z}/n\mathbb{Z})^2$.
Donc $|\mathbb{Z}[\sqrt{d}]/(n)| = |(\mathbb{Z}/n\mathbb{Z})|^2 = n^2$, ce qui conclut la preuve.

3.5 Existence d'une solution non triviale

Nous disposons maintenant de tous les outils nécessaires pour prouver le théorème suivant.

Théorème : Pour tout entier naturel non nul d qui n'est pas un carré, l'équation de Pell-Fermat possède une solution entière non triviale.

Preuve : Il s'agit de montrer l'existence d'un élément $z \neq \pm 1$ de $\mathbb{Z}[\sqrt{d}]$.
En effet, rappelons que $S_d \cong N_1(d)$, ce qui signifie que la correspondance entre une solution (x,y) de S_d et z est unique.

On se donne deux entierx $n > 2\sqrt{d} + 1$ et $m = n!$.
(1) On montre que $(m) \subset (\alpha)$.
Pour tout $\alpha \in \mathbb{Z}[\sqrt{d}]$ tel que $|N(\alpha)| \leq n$, $N(\alpha)$ est un entier qui divise $m = n!$ puisque c'en est l'un des facteurs (au signe près).
Ecrivons $m = N(\alpha) \times k$ pour $k \in \mathbb{Z}$. Alors $(m) \subset N(\alpha)$ car $\forall u \in \mathbb{Z}[\sqrt{d}], mu = N(\alpha) \times k \times u \in (N(\alpha))$
D'autre part, $N(\alpha) = \alpha\sigma(\alpha) \in (\alpha)$, ce qui entraîne avec ce que l'on vient de montrer que $(m) \subset (\alpha)$
(2) On applique le lemme de cardinalité qui montre que $\mathbb{Z}[\sqrt{d}]/(m)$ est fini et de cardinal $m^2 = (n!)^2$ et possède donc en particulier un **nombre fini d'idéaux**.
Or nous disposons du lemme suivant :
Pour chaque $m \in \mathrm{N}^*$, il existe une bijection entre les idéaux de $\mathbb{Z}[\sqrt{d}]/(m)$ et les idéaux de $\mathbb{Z}[\sqrt{d}]$ contenant (m).
En particulier, il y a donc autant d'idéaux de $\mathbb{Z}[\sqrt{d}]/(m)$ que d'idéaux de $\mathbb{Z}[\sqrt{d}]$ contenant (m).
Donc il existe un nombre fini d'idéaux de $\mathbb{Z}[\sqrt{d}]$ contenant (m).
(3) D'après le corollaire du théorème de Dirichlet, il y a donc une infinité d'éléments $\alpha \in \mathbb{Z}[\sqrt{d}]$ qui satisfont les deux conditions imposées telles que $(m) \subset (\alpha)$, cette inclusion étant vraie pour n'importe quel élément $\alpha \in \mathbb{Z}[\sqrt{d}]$.
Et en particulier, elle est vraie pour **une infinité d'idéaux contenant** (m) dont un élément α satisfait

$$\begin{cases} \alpha > 2\sqrt{d} - 1 \\ \text{ et} \\ |N(\alpha)| < 2\sqrt{d} + 1 \end{cases}$$

pour **un nombre fini d'idéaux contenant** (m).
(4) Nous appliquons le principe des tiroirs comme ci-dessous.
Les tiroirs sont les idéaux de $\mathbb{Z}[\sqrt{d}]$ contenant (m), et les chaussettes sont les éléments $\alpha \in \mathbb{Z}[\sqrt{d}]$ satisfaisant les deux conditions décrites ci-dessus. Il y en a une infinité, donc il existe deux éléments $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ tels que $\alpha, \beta > 2\sqrt{d} - 1$ et $(\alpha) = (\beta)$.
On obtient que α et β sont associés d'après le lemme de la section 3.4, ce qui

signifie littéralement que

$$\exists u \in (\mathbb{Z}[\sqrt{d}])^\times, \beta = u\alpha.$$

Or $N((\mathbb{Z}[\sqrt{d}])^\times) = \{\pm 1\}$ Mais d'après la troisième propriété de la norme N, cela signifie que $N(u) = \pm 1$. D'où $N(u^2) = N(u)N(u) = (\pm 1)^2 = 1$.
Donc $v = u^2$ est un élément de $\mathbb{Z}[\sqrt{d}]$ de norme 1. Il définit donc une solution entière de l'équation de Pell-Fermat.
(5) Il nous reste à montrer qu'il ne fournit pas une solution triviale (ie. montrer que $v \neq \pm 1$).
Comme $v = u^2 \geq 0$, on a évidemment $v \neq -1$.
Si $v = 1$, alors on aurait $\alpha = \pm\beta$, ce qui n'est pas possible car ils vérifient $\alpha, \beta > 2\sqrt{d} - 1 \ > 2 - 1 > 0$ puisque $d > 1$ (le cas où d est le carré d'un entier ayant déjà été résolu).
En particulier, ils sont strictement positifs et également distincts.
Ainsi, en notant $v = x + y\sqrt{d}$, le couple (x, y) est une solution non triviale de l'équation de Pell-Fermat. Ce qu'il fallait démontrer.

3.6 Conclusion

En comparant avec l'étude des solutions réalisée dans le premier chapitre, l'équation de Pell-Fermat possède une solution entière non triviale si et seulement si $d = -1$, ou si $d > 0$ et n'est pas le carré d'un entier.

Chapitre 4

Structure des solutions de l'équation de Pell-Fermat

Introduction

Nous cherchons dans ce chapitre une façon de caractériser toutes les solutions de l'équation de Pell-Fermat, ce qui nous amène à caractériser le groupe $N_1(d)$. Nous commençons notre étude par la remarque suivante :

Remarque : Pour toute solution (x, y), nous disposons de quatre solutions : (x, y), $(-x, y)$, $(x, -y)$ et $(-x, -y)$ puisque seul le carré de ces nombres intervient dans l'équation. De ce fait, nous pouvons déterminer toutes les solutions de l'équation de Pell-Fermat en étudiant uniquement les solutions de la forme (x, y) où x et y sont positifs.

4.1 Définition et propriétés de la solution minimale

Nous commençons ce chapitre par une définition centrale dans notre étude. On rappelle que $S_d = \{(x, y) \mid x^2 - dy^2 = 1\}$.

Définition : La solution minimale est un couple $(x, y) \in S_d$ vérifiant : $\begin{cases} y \text{ est minimal} \\ x, y > 0 \end{cases}$
Nous emploierons la même terminologie pour désigner l'unique élément de $N_1(d)$ qui lui est associé.

4.1.1 Les trois définitions de la solution minimale

Dans cette section souhaitons prouver le lemme suivant fournissant trois définitions de la solution minimale.

Lemme : Soit $z = x+y\sqrt{d}$ où $x, y > 0$ un élément de $\mathbb{Z}[\sqrt{d}]$. Il est équivalent :
(1) $z = x + y\sqrt{d}$ est minimal
(2) x est minimal
(3) y est minimal

Preuve : Soient $z = x + y\sqrt{d}$ et $z' = x' + y'\sqrt{d}$ tels que x, y, x', y' sont des réels positifs.
Montrons que (2) $\Leftrightarrow$ (3)
Nous avons

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

Ce qui entraîne en réordonnant les termes $(x - x')^2 = d(y^2 - y'^2)$. Soit

$$(x - x')(x + x') = d(y - y')(y + y')$$

Et par hypothèse, nous avons $d > 0$, $x + x' \geq 0$ et $y + y' \geq 0$, de sorte que le signe de chaque membre de l'égalité est déterminé par $x - x'$ et $y - y'$
D'où

$$x - x' \geq 0 \Leftrightarrow y - y' \geq 0$$

ce qui entraîne que la minimalité de x équivaut à celle de y.
L'implication (3) $\Rightarrow$ (1) est de ce fait évidente puisque la minimalité de y entraîne celle de x et donc celle de $z = x + y\sqrt{d}$.
L'implication réciproque provient de la définition de la solution minimale.

4.1.2 Une quatrième définition de la solution minimale

Nous avons besoin d'un résultat plus général sur les éléments de $\mathbb{Z}[\sqrt{d}]$ pour fournir une nouvelle caractérisation de la solution minimale. Intéressons-nous au résultat suivant.

Lemme : Soit $z = x+y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Les assertions suivantes sont équivalentes.
(1) x et y sont strictement positifs.
(2) $z > \sqrt{|N(z)|}$

Preuve : Commençons par prouver l'implication (1) $\Rightarrow$ (2).
Nous partons donc de $z = x + y\sqrt{d}$ où x et y sont strictement positifs, ce qui entraîne immédiatement que $z > 0$.
On a donc $z > z - 2y\sqrt{d}$.

De plus, $x = z - y\sqrt{d} > 0$, d'où $2z > 2y\sqrt{d}$, ce qui se traduit par $z - y\sqrt{d} > -z$. Nous venons de montrer que

$$z > z - 2y\sqrt{d} > -z$$

ce qu'on peut réécrire

$$z > |z - 2y\sqrt{d}| = |x - y\sqrt{d}| = |\sigma(z)|$$

En multipliant chaque membre par $|z| = z > 0$

$$z^2 > |z\sigma(z)| = |N(z)|$$

d'où par positivité de z et $|N(z)|$

$$z > \sqrt{|N(z)|}$$

Il ne reste plus qu'à montrer l'implication réciproque.
Nous pouvons commencer par remarquer que si $z > \sqrt{|N(z)|}$ alors x **et** y **sont non nuls**. En effet, si par l'absurde ce n'était pas le cas, alors $xy = 0$ et

$$z^2 = x^2 + dy^2 + 2xy\sqrt{d} = x^2 + dy^2 > \sqrt{|N(z)|}^2 = |x^2 - dy^2|$$

ce qui entraîne, en utilisant l'inégalité triangulaire inversée

$$|2y^2| \geq |x^2 + dy^2| - |x^2 - dy^2| > 0$$

Donc $y \neq 0$ ce qui entraîne $x = 0$. On a donc :

$$z^2 = dy^2 > |-dy^2| = dy^2$$

ce qui est absurde.
Par ailleurs, puisque $N(z) = x^2 - dy^2$, la norme de dépend pas du signe de x et y. Ainsi, les éléments de $S = \{\pm z, \pm\sigma(z)\} = \{\pm x \pm y\sqrt{d}\}$ ont tous la même norme. Notons $t = \max(S) = |x| + |y|\sqrt{d}$.
Montrons que $z = t$. Par l'absurde, supposons que $z \neq t$. Alors par positivité de z, on aurait $z = |x| - |y|\sqrt{d}$ ou $z = -|x| + |y|\sqrt{d}$. Dans les deux cas, on remarque que

$$|\sigma(z)| = |x| + |y|\sqrt{d} = t$$

Ce qui montre que

$$|N(z)| = |z\sigma(z)| = z|\sigma(z)| = zt > \sqrt{|N(z)|}t$$

Ceci entraîne en divisant par $\sqrt{|N(z)|} > 0$ (puisque x et y sont non nuls).

$$z > \sqrt{|N(z)|} > t$$

Ce qui contredit la maximalité de t. On en déduit $z = t$. Cela s'écrit $z = x + y\sqrt{d} = |x| + |y|\sqrt{d}$ et par l'unicité de cette écriture, on en déduit que $x = |x| > 0$ et $y = |y| > 0$. Ce qui conclut.

Nous déduisons des lemmes précédents la proposition suivante qui occupe un rôle central dans la preuve qui suit.

Proposition : La solution minimale (x, y) est le plus petit élément de $N_1(d)$ strictement supérieur à 1.

4.2 Structure du groupe $N_1(d)$

Tous les outils sont maintenant à notre disposition pour prouver le théorème ci-dessous.

Théorème Le groupe multiplicatif $(N_1(d), \times)$ est engendré par -1 et par la solution minimale.
Ce que nous pouvons traduire comme suit en notant $z_0 = x_0 + y_0\sqrt{d} \in N_1(d)$ la solution minimale : Pour tout $z \in N_1(d)$, il existe $(a, b) \in \mathbb{Z}^2$ tel que $z = (-1)^a z_0^b$.

Preuve :

Nous avons précédemment établi que chaque solution (x, y), nous donne quatre solutions : (x, y), $(-x, y)$, $(x, -y)$ et $(-x, -y)$, ce que nous pouvons traduire comme suit en utilisant l'isomorphisme $S_d \cong N_1(d)$
Pour tout $z \in \mathbb{Z}[\sqrt{d}]$,

$$\{z, \sigma(z), -z, -\sigma(z)\} \subset \mathbb{Z}[\sqrt{d}]$$

Au moins l'un de ces nombres est strictement plus grand que 1 car l'unique couple $(x, y) \in S_d$ qui lui est associé vérifie $x > 0$, $y > 0$.
Soit $z_0 = x_0 + y_0\sqrt{d} \in N_1(d)$ la solution minimale et $z = x + y\sqrt{d} \in N_1(d)$.

Ainsi, nous pouvons pour le moment nous limiter au cas plus commode où $x > 0$ et $y > 0$ ce qui entraîne immédiatement que $z > 1$.
Par minimalité de z_0, on a $z \geq z_0$.
Mais puisque $z_0 > 1$, nous avons $(z_0^n) \underset{n\to+\infty}{\longrightarrow} +\infty$ comme suite géométrique.
Cette limite s'écrit :

$$\exists N \in \mathbb{N}, \forall n \geqslant N, z_0^n > z$$

Mais alors $A = \{n \in \mathbb{N} \mid z_0^n > z\}$ est une partie non vide de $\mathbb{N}$. En tant que tel, elle admet un plus petit élément noté n_0.
Et puisque $z \geq z_0$ et $z > 1$, 1 et 0 ne sont pas dans A donc $n_0 > 1$.
Par minimalité de n_0, $n_0 - 1 \notin A$ d'où

$$z_0^n > z \geq z_0^{n_0-1}$$

Posons $n = n_0 - 1 > 0$. Nous pouvons la réécrire $z_0^{n+1} > z \geq z_0^n$.
Multiplions par $\sigma(z_0)^n$: $z_0 \times (\sigma(z_0)z_0)^n = \sigma(z_0)^n z_0^{n+1} > \sigma(z_0)^n z \geq (\sigma(z_0)z_0)^n$
Ce qui équivaut à : $z_0 N(z_0)^n > \sigma(z_0)^n z \geq N(z_0)^n$.
Soit en divisant par $N(z_0)^n = 1^n = 1$:

$$z_0 > \sigma(z_0)^n z \geq 1$$

Remarquons que $\sigma(z_0)^n z \in N_1(d)$ puisque $N(\sigma(z_0)^n z) = N(\sigma(z_0))^n N(z)$ par multiplicativité de la norme. Ceci vaut $N(\sigma(z_0))^n N(z) = 1^n \times 1 = 1$

De ce fait, si on avait $z_0 > \sigma(z_0)^n z > 1$, alors comme élément de $N_1(d)$, $\sigma(z_0)^n z$ contredirait la minimalité de z_0 ! On en déduit finalement que

$$\sigma(z_0)^n z = 1$$

Il ne s'agit plus que de réécrire $z = \frac{1}{\sigma(z_0)^n} = \sigma(\sigma(z_0))^n = z_0^n$.

Pour conclure, il suffit de remarquer que chaque élément de $\{z, \sigma(z), -z, -\sigma(z)\}$ s'écrit comme $\pm z_0^{\pm 1}$, ce qui permet d'étendre le résultat trouvé à tout élément de $N_1(d)$ avec

$$z = \pm z_0^{\pm n}$$

ce qui montre exactement le résultat souhaité.

Corollaire : $N_1(d) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

Preuve : On note $z \in N_1(d)$ la solution minimale.
L'application

$f : \begin{cases} (Z/2Z) \times Z \to N_1(d) \\ (a,b) \mapsto (-1)^a z^b \end{cases}$ est un morphisme de groupes (vérification immédiate).

(1) La surjectivité de f découle directement de ce qui vient d'être montré.

(2) Il s'agit de montrer l'injectivité de f.

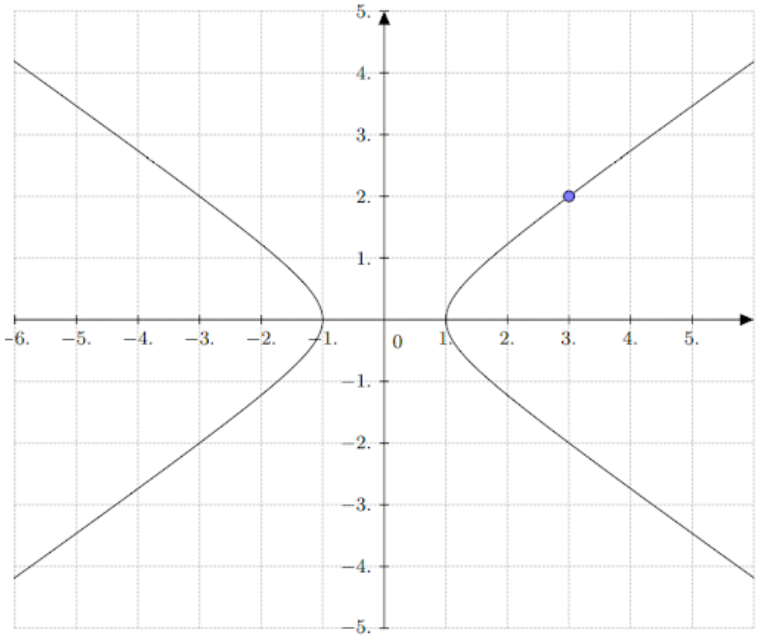
$$(a,b) \in \ker(f) \Rightarrow \text{b=0 et a est pair.}$$

Or a $\in \mathbb{Z}/2\mathbb{Z}$ donc $b = 0$ et $a = 0$, ainsi f est injective.
f est donc un isomophisme, ce qui implique que $N_1(d) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$

4.3 Approche géométrique de l'équation de Pell-Fermat

Nous terminons cette exposé par une interprétation graphique de l'équation. L'équation de Pell-Fermat $x^2 - dy^2 = 1$ dessine une figure dans le plan appelée une hyperbole pour $d \in \mathbb{Z}$ fixé. **Les solutions de cette équation sont les coordonnées des points à coordonnées entières de la courbe.**

Nous avons vu qu'à partir d'une solution à coordonnées positives (x, y), nous obtenons quatre solutions : (x, y), $(-x, y)$, $(x, -y)$ et $(-x, -y)$, ce qui explique la symétrie de la courbe par rapport aux deux axes.
Plus précisément, l'hyperbole admet une symétrie par rapport à l'axe des ordonnées (qui envoie le point de coordonnées (x, y) sur celui de coordonnées $(-x, y)$, une symétrie par rapport à l'axe des abscisses (qui envoie (x, y) sur $(x, -y)$), ainsi que la composée de ces deux symétries, qui est la symétrie centrale par rapport à l'origine (qui envoie (x, y) sur $(-x, -y)$)



L'hyperbole $x^2 - 2y^2 = 1$, avec un point entier (3,2).

Les solutions triviales $(1, 0)$ et $(-1, 0)$ correspondent aux points d'intersection de la courbe avec l'axe des abscisses. Les points à coordonnées entières positives sont situés sur le quart supérieur droit de l'hyperbole. Ce sont ceux qui définissent une solution (x, y) tels que $x > 0$ et $y > 0$. Nous remarquons que ces solutions vérifient bien $x > 1$. Par ailleurs, nous retrouvons la solution minimale qui correspond au **point à coordonnées entières le plus proche de l'origine dans le quart supérieur droit**.
Sur le graphique de l'hyperbole ci-dessus, nous voyons que c'est le point $(3, 2)$.

Bibliographie

[Zapponi, 2021] Zapponi, L. (2021). ***Pell-Fermat****, notes de cours, pages 1-28.*

[Bilu,2015] Bilu, M. (2015). ***Fractions continues****, notes de cours, pages 15-19.* France, Grenoble.

[Pierron] Pierron, T. ***Théorie des nombres****, notes de cours, pages 37-50.* ENS Ker Lann, France, Rennes.

[Hindry,2005] Hindry, M. (2005). ***Cours d'arithmétique (M1)****, notes de cours, pages 41-48.* Université Denis Diderot, France, Paris 7.

[Von Buhren] Von Buhren, J. ***L'équation de Pell-Fermat****, Préparation à l'aggrégation.* Université de Strasbourg, France.

[Edditions-Ellipses], Edditions-Ellipses. ***Anneaux, morphismes, et idéaux****, notes de cours, pages 1,4.*