# Feuille d'exercices 2

*Remarque :* Tous les exercices ne seront pas traités en séance de TD, j'indiquerai au fur et à mesure sur la page du forum (http ://cours-jussieu-nombres.monforum.com/cours-et-td-2009-vf7.html) les exercices que nous aurons abordés.

## 1 Equations diophantiennes sur $\mathbb{C}[X]$

Du point de vue de l'arithmétique tout est parfait puisque $\mathbb{C}[X]$ est principal et que les irréductibles sont parfaitement connus : en illustration donnez une preuve arithmétique de l'équation de Fermat sur $\mathbb{C}[X]$.

**Exercice 1.1.** *Soient $n > 2$ et $x, y, z$ trois polynômes de $\mathbb{C}[X]$ premiers entre eux ; montrez que l'équation $x^n + y^n = z^n$ implique que les trois polynômes sont des constantes.*

Un autre avantage des anneaux de polynômes au delà de l'aspect arithmétique favorable, est que l'on dispose de la dérivation. Le résultat classique est le fameux théorème de Mason.

**Exercice 1.2.** *Les polynômes de cet exercice seront à coefficients complexes, i.e. des éléments de $\mathbb{C}[X]$. Pour $P \in \mathbb{C}[X]$, on note $n_0(P)$ le nombre de ses racines distinctes qui est donc le degré du polynôme $N_0(P) = \frac{P}{P \wedge P'}$.*

*(1) Soient $a(x)$, $b(x)$ et $c(x)$ des polynômes premiers entre eux deux à deux tels que $a + b + c = 0$.*

*(a) On pose $f = \frac{a}{c}$ et $g = \frac{b}{c}$ qui sont donc des fractions rationnelles. Montrez que l'on a la relation*

$$\frac{b}{a} = \frac{g}{f} = -\frac{f'/f}{g'/g}.$$

*(b) De l'égalité $\frac{b}{a} = -\frac{N_0(abc)f'/f}{N_0(abc)g'/g}$, montrez que $\deg a$ et $\deg b$ sont inférieurs strictement à $n_0(abc)$.*

*(c) Déduisez de ce qui précède que $\max\{\deg a, \deg b, \deg c\} \leq n_0(abc) - 1$ : c'est le **théorème de Mason**.*

*(2) Soient $f, g, h$ des polynômes premiers entre eux dont un au moins n'est pas constant. Montrez que pour $n \geq 3$ l'égalité $f^n + g^n = h^n$ est impossible.*

*(3) Soient $\alpha, \beta, \gamma$ des entiers tels que $2 \leq \alpha \leq \beta \leq \gamma$. Montrez alors que l'équation $f^\alpha + g^\beta = h^\gamma$ n'a pas de solutions premières entre elles sauf pour $(\alpha, \beta, \gamma)$ égal à*

$$(2, 2, \gamma), \quad (2, 3, 3), \quad (2, 3, 4), \quad (2, 3, 5).$$

*(4) Pour $m, n \geq 2$, montrez que si l'équation $x^n - y^m = 1$ possède des solutions dans $\mathbb{C}(x)$ alors $m = n = 2$.*

**Exercice 1.3.** *Problème de Waring sur $\mathbb{C}[X]$ : il s'agit pour $n$ fixé de trouver l'entier $k(n)$ minimal parmi les $k$ tels que tout $g \in \mathbb{C}[x]$ peut s'écrire sous la forme*

$$g = f_1^n + \cdots + f_k^n.$$

*(1) Montrez qu'il suffit de traiter le cas de $g(x) = x$.*

*(2) Montrez que $k(2) = 2$.*

*(3) Soit désormais $n \geq 3$ ; montrez en raisonnant par l'absurde que $k(n) \geq 3$.*

*(4) Notons $\Delta f(x) = f(x+1) - f(x)$ et $\Delta^p f = \Delta\Big(\Delta^{p-1} f\Big)$. En utilisant que $\Delta^{n-1}(x^n)$ est de la forme $ax + b$, montrez que $k(n) \leq n$.*

*(5) Dans cette question nous allons montrer que $n < k^2(n) - k(n)$. Pour $f_1, \cdots, f_n$ des fonctions d'une variable réelle $t$, dérivables $n - 1$ fois sur un certain intervalle, leur wronskien $W(f_1, \cdots, f_n)$ est la fonction*

$$W(f_1, \cdots, f_n)(t) = \begin{vmatrix} f_1(t) & f_2(t) & \cdots & f_n(t) \\ f_1'(t) & f_2'(t) & \cdots & f_n'(t) \\ \vdots & \vdots & & \vdots \\ f_1^{(n-1)}(t) & f_2^{(n-1)}(t) & \cdots & f_n^{(n-1)}(t) \end{vmatrix}.$$

***On admet** que si $f_1, \cdots, f_n$ sont des fonctions polynomiales sur $\mathbb{C}$ alors $W(f_1, \cdots, f_n) = 0$ sur un intervalle d'intérieur non vide si et seulement si la famille $(f_1, \cdots, f_n)$ est liée.*

(a) *Soit* $x = f_1^n(x) + \cdots + f_k^n(x)$ *avec* $f_i \in \mathbb{C}[x]$ *et* $k$ *minimal. Considérons les wronskiens* $W_1 = W(f_1^n, \cdots, f_k^n)$ *et* $W_2 = W(x, f_2^n, \cdots, f_k^n)$*. Montrez que* $W_1 = W_2$ *n'est pas le polynôme nul.*

(b) *Montrez que* $W_1$ *est divisible par* $\prod_{i=1}^k f_i^{n-k+1}$.

(c) *Montrez que*

$$\deg W_2 \leq 1 + n\sum_{i=2}^k \deg f_i - 1 - 2 - \cdots - (k-1) = n\sum_{i=2}^k \deg f_i - \frac{k(k-1)}{2} + 1.$$

(d) *Déduire de (b) et (c) que* $n \deg f_1 \leq (k-1)\sum_{i=1}^k \deg f_i - \frac{k(k1)}{2} + 1$.

(e) *Montrez que* $n < k^2(n) - k(n)$.

*Indication : supposez que* $f_1$ *est de degré maximal parmi les* $f_i$.

# 2 Des exemples simples d'équations diophantiennes sur $\mathbb{Z}$

## 2.1 Le cas linéaire

**Exercice 2.1.** *(1) Trouvez toutes les solutions entières de* $ax + by = c$.

*(2) Pour* $a \wedge p = 1$*, montrez que l'équation* $x^n \equiv a \mod p$ *possède* $n \wedge (p-1)$ *solutions si et seulement si* $a^{\frac{p-1}{n \wedge (p-1)}} \equiv 1 \mod p$ *et sinon elle n'en possède aucune.*

*(3) Montrez que le système de congruence* $x \equiv a \mod n$ *et* $x \equiv b \mod m$ *n'a de solutions que si* $n \wedge m$ *divise* $a - b$.

*(4) En ce qui concerne les solutions positives montrez que pour* $a \wedge b = 1$ *si* $m + n = ab - a - b$ *alors exactement un des paramètres* $m, n$ *possède des solutions dans* $\mathbb{N}$*. En particulier si* $m > ab - a - b$ *alors l'équation* $ax + by = m$ *a des solutions* $(x, y) \in \mathbb{N}^2$ *; pour* $m = ab - a - b$ *elle n'en a pas et pour* $m \leq ab - a - b$ *exactement la moitié de ces* $m$ *ont de solutions.*

**Exercice 2.2.** *(1) Résolvez dans* $\mathbb{Z}^n$ *l'équation* $a_1x_1 + \cdots + a_nx_n = b$.

*(2) Etudiez l'équation* $AX = B$ *où* $A \in \mathbb{M}_{m,n}(\mathbb{Z})$ *et* $B \in \mathbb{M}_{n,1}(\mathbb{Z})$.

**Exercice 2.3.** *Montrez que le nombre de solutions entières positives de l'équation diophantienne*

$$x + 2y + 3z = n$$

*est égal à l'entier le plus proche de* $\frac{(n+3)^2}{12}$.

**Exercice 2.4.** *Montrez que le nombre de solutions entières positives des équations diophantiennes suivantes*

$$x + 2y = n, \quad 2x + 3y = n - 1, \quad 3x + 4y = n - 2, \cdots, nx + (n+1)y = 1, \quad (n+1)x + (n+2)y = 0$$

*est égal à* $n + 1$.

**Exercice 2.5.** *Soient* $a_1, \cdots, a_l$ *des entiers positifs premiers entre eux dans leur ensemble. Soit* $A_n$ *le nombre de solutions entières positives de*

$$a_1x_1 + a_2x_2 + \cdots + a_lx_l = n$$

*(1) Montrez que*

$$\lim_{n\to\infty} \frac{A_n}{n^{l-1}} = \frac{1}{a_1 \cdots a_l (l-1)!}.$$

*(2) Supposons en outre que les* $a_i$ *sont premiers entre eux deux à deux. Montrez alors que*

$$A_n = P(n) + Q_n$$

*où* $P(x)$ *est un polynôme à coefficients rationnels de degré* $l - 1$ *et où la suite* $Q_n$ *est périodique de période* $a_1 \cdots a_l$.

*(3) Dans le cas $l = 2$ où $a_1 = a$ et $a_2 = b$ sont premiers entre eux, montrez que*

$$A_n \leq 1 \text{ quand } n < ab,$$
$$A_n \geq 1 \text{ quand } n > ab - a - b,$$

*et qu'en outre on a :*
- $A_{ab} = 2$,
- $A_{ab-a-b} = 0$,
- $A_{n+ab} = A_n + 1$,
- $A_n$ *est égal à* $\lfloor \frac{n}{ab} \rfloor$ *ou* $\lfloor \frac{n}{ab} \rfloor + 1$.

### 2.2 Utilisation de congruences

**Exercice 2.1.** *Montrez que*
*(1)* $y^2 = 41x + 3$ *n'a pas de solutions car* $(\frac{3}{41}) = -1$ *;*
*(2)* $y^2 = x^3 + 7$ *n'a pas de solutions entières ;*

*Remarque :* $y^3 = px + 2$ avec $p \equiv 1 \mod 3$ a une solution si et seulement s'il existe a, $b \in \mathbb{Z}$ tels que $p = x^2 + 27y^2$ ; la preuve est cette fois plus difficile et repose sur le résultat suivant : $p$ s'écrit sous la forme $x^2 + 27y^2$ si et seulement si 2 est un cube modulo $p$.

### 2.3 Extension de corps, d'anneau des entiers principal

L'exercice suivant est plus classique en remplaçant $i\sqrt{2}$ par $i$ ; dans les deux situations les preuves sont strictement identiques.

**Exercice 2.1.** *Soit* $A = \mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \ / \ (a, b) \in \mathbb{Z}^2\}$. *On définit pour* $z = a + ib\sqrt{2} \in A$, $N(z) = a^2 + 2b^2$.
*(a) Montrez que $B$ est euclidien et donc factoriel.*
*(b) Soient* $(x, y) \in \mathbb{Z}^2$, *vérifiant l'équation* $y^2 + 2 = x^3$. *Montrez que $x$ est impair puis que dans $B$,* $y + i\sqrt{2}$ *et* $y - i\sqrt{2}$ *sont premiers entre eux. En déduire qu'il existe* $(a, b) \in \mathbb{Z}^2$ *tels que* $x = a^2 + 2b^2$ *et* $y + i\sqrt{2} = (a + ib\sqrt{2})^3$, *puis décrire les solutions de l'équation précédente.*
*(c) Étudiez comme dans l'exercice précédent l'ensemble* $S = \{n \in \mathbb{N} \ / \ \exists (x, y) \in \mathbb{Z}^2, \ n = x^2 + 2y^2\}$.
*Indication : on utilisera que* $-2$ *est un carré dans* $\mathbb{Z}/p\mathbb{Z}$ *si et seulement si* $p \equiv 1, 3 \mod 8$.
*(d) Étudiez de même l'ensemble* $\{n \in \mathbb{Z} \ / \ \exists (x, y) \in \mathbb{Z}^2, \ n = x^2 - 2y^2\}$.

### 2.4 Méthode de descente

**Exercice 2.1.** *Soit l'équation* $x^4 + y^4 = z^2$.
*(1) Montrez que si* $(x, y, z)$ *est une solution avec* $x \wedge y \wedge z = 1$ *alors* $z > 0$ *$y$ pair et $x$ impair*
*(2) On suppose* $y \neq 0$ *et on écrit* $y^4 = (z - x^2)(z + x^2)$. *Montrez que* $(z - x^2) \wedge (z + x^2) = 2$ *et en déduire que*

$$(z - x^2, z + x^2) = (2a^4, 8b^4) \text{ ou } (8b^4, 2a^4), \quad a \equiv 1 \mod 2, \quad a \wedge b = 1, \quad a > 0.$$

*(3) Montrez que le cas* $(z - x^2, z + x^2) = (2a^4, 8b^4)$ *est impossible.*
*(4) Construisez une solution* $(c, d, a)$ *de l'équation telle que* $0 < a < z$ *et concluez.*

### 2.5 Equations possédant une infinité de solutions

**Exercice 2.1.** *Le plan* $\mathcal{P}$ *étant rapporté à un repère orthonormal* $(O, \vec{u}, \vec{v})$, *on considère l'hyperbole* $\mathcal{H}$ *d'équation* $x^2 - 3y^2 = 1$ *et on désigne par* $\mathfrak{S}$ *l'ensemble des points du plan dont les deux coordonnées sont des éléments de* $\mathbb{Z}$. *On se propose d'étudier l'ensemble* $\mathcal{H} \cap \mathfrak{S}$.
*(1) A tout point $M$ de coordonnées* $(x, y)$ *dans* $(O, \vec{u}, \vec{v})$, *on associe son affixe* $z = x + iy \in \mathbb{C}$. *On définit une application* $f : \mathbb{C} \to \mathbb{C}$ *par* $f(z) = (2 - i)z + 2i\bar{z}$. *A $f$ on associe l'application* $F : \mathcal{P} \to \mathcal{P}$ *qui au point d'affixe $z$ associe* $M' = F(M)$ *d'affixe* $z' = f(z)$.
*(i) Montrez que $F$ est une application affine et bijective qui conserve les aires des triangles. Est-ce une isométrie ?*

*(ii) Montrez que $M$ appartient à $\mathcal{H}$ (resp. $\mathfrak{S}$) si et seulement si $M'$ aussi.*

*(2) On construit par récurrence une suite de points $(A_n)_{n\in\mathbb{N}}$ en posant pour tout $n$ : $A_{n+1} = F(A_n)$, $A_0$ étant le point de coordonnées $(1, 0)$.*

*(i) Calculez les coordonnées de $A_1$ et $A_2$ puis montrez que pour tout $n$, $A_n \in \mathcal{H} \cap \mathfrak{S}$.*

*(ii) Quels sont les points de $\mathfrak{S}$ situés sur l'arc $[A_0, A_1]$ de $\mathcal{H}$ ?*

*(3) On définit sur $\mathcal{H}$ une opération $*$ ainsi : $M$ et $N$ étant deux points de $\mathcal{H}$, on leur associe la droite $D_{M,N}$ issue de $A_0$ et parallèle à la droite $(MN)$ (ou à la tangente en $M$ à $\mathcal{H}$ si $M = N$). Dans le cas où $D_{M,N}$ est tangente à $\mathcal{H}$ en $A_0$, on pose $M * N = A_0$ et sinon $M * N$ est le second point de rencontre de $D_{M,N}$ avec $\mathcal{H}$, cf. la figure 1*

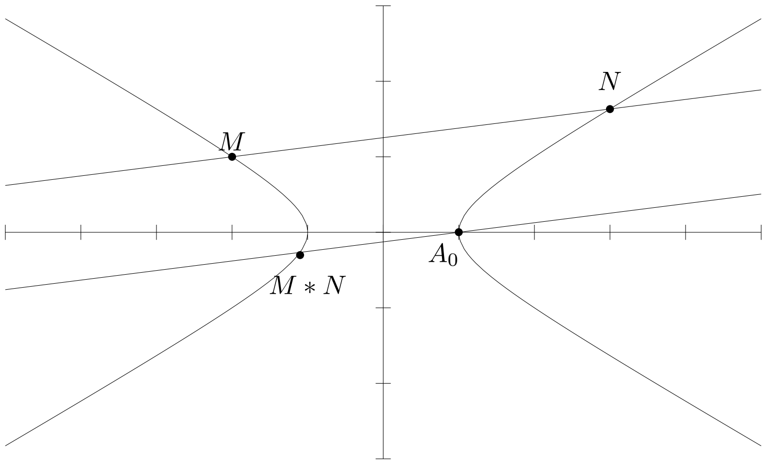


FIGURE 1 – Loi de groupe sur une hyperbole

*(i) Montrez qu'il existe un repère $\mathcal{R}$ de $\mathcal{P}$ dans lequel $\mathcal{H}$ a pour équation $XY = 1$. Exprimez alors dans ce repère l'abscisse de $M * N$ en fonction de celle de $M$ et $N$. En déduire que $(\mathcal{H}, *)$ est un groupe isomorphe au groupe multiplicatif $(\mathbb{R}^*, \times)$.*

*(ii) Montrez que pour tout $M \in \mathcal{H}$, $F(M) = A_1 * M$ et calculez les coordonnées $(X_n, Y_n)$ de $A_n$ dans $\mathcal{R}$ en fonction de $X_1$ et $n$.*

*(iii) Montrez que la tangente en $A_n$ à $\mathcal{H}$ est parallèle à la droite $(A_{n-1}A_{n+1})$ puis calculez l'aire du triangle $A_{n-1}A_nA_{n+1}$.*

*(iv) Prouvez que $M$ est un point de l'arc $[A_n, A_{n+1}]$ de $\mathcal{H}$ si et seulement si $M' = A_1 * M$ appartient à l'arc $[A_{n+1}, A_{n+2}]$ de $\mathcal{H}$. Décrivez alors l'ensemble $\mathcal{H} \cap \mathfrak{S}$.*

*(4) Donnez tous les couples $(x, y)$ de nombres entiers naturels solutions de l'équation $x^2 - 3y^2 = 1$.*

**Exercice 2.2.** *Étude de l'équation de Pell-Fermat : $x^2 - Ny^2 = 1$.*

*(i) Traitez le cas $N \leq 0$.*

*(ii) Montrez que dans le cas où $N$ est un carré parfait, les solutions triviales $x = \pm 1, y = 0$ sont les seules.*

*(iii) On suppose donc $N > 1$ et $N$ n'est pas un carré parfait. En utilisant l'anneau $\mathbb{Z}[\sqrt{N}]$, montrez l'égalité :*

$$(x_1^2 - Ny_1^2)(x_2^2 - Ny_2^2) = (x_1x_2 + Ny_1y_2)^2 - N(x_1y_2 + x_2y_1)^2$$

*En déduire que s'il existe un solution non triviale $(x_0, y_0)$ à l'équation de Pell-Fermat, alors il en existe une infinité $(x_n, y_n)$ définie par récurrence :*

$$\begin{cases} x_{n+1} = x_0x_n + Ny_0y_n \\ y_{n+1} = x_0y_n + x_ny_0 \end{cases}$$

*Calculez par exemple pour $N = 2$, les 3 premiers termes de cette suite en remarquant que $(3, 2)$ est solution.*

*(iv) Montrez que pour $(x_1, y_1)$ et $(x_2, y_2)$ des solutions positives de l'équation, les équivalences*

$$x_1 < x_2 \Leftrightarrow y_1 < y_2 \Leftrightarrow (x_1 + y_1\sqrt{N}) < (x_2 + y_2\sqrt{N})$$

*En déduire que s'il existe des solutions non triviales alors il existe une solution minimale $(x_0, y_0)$ pour une relation d'ordre que l'on définira. Montrez ensuite que l'ensemble des solutions sont les $(x_n, y_n)$ définis ci-dessus.*

(v) *On veut montrer l'existence d'une solution non triviale. Montrez qu'il existe une infinité de rationnels $p/q$ tels que $|\sqrt{N} - p/q| < 1/q^2$.*
*Indication : commencez par remarquer que $p$ ou $p-1$ est la partie entière de $q\sqrt{N}$, puis appliquez le principe des chaussettes et des tiroirs ($n+1$ chaussettes rangées dans $n$ tiroir, implique qu'un tiroir contient au moins deux chaussettes), où les chaussettes sont les $n\sqrt{N} - [n\sqrt{N}]$ pour $0 \leq n \leq q$ et les tiroirs sont les intervalles $[k/q, (k+1) : q]$ pour $0 \leq k < q$.*
*En déduire qu'il existe une infinité de couples $(p, q) \in \mathbb{N}^2$ premiers entre eux tels que $-1-2\sqrt{N} < p^2 - Nq^2 < 1+2\sqrt{N}$. En utilisant à nouveau le principe des tiroirs, montrez qu'il existe un entier $l < 1+2\sqrt{N}$, $p_1 \equiv p_2 \mod l$, $q_1 \equiv q_2 \mod l$ tels que $p_1^2 - Nq_1^2 = p_2^2 - Nq_2^2 = \pm l$, et en déduire l'existence d'une solution non triviale.*

*Remarque :* d'autres équations que nous traiterons plus loin :
- *courbes elliptiques* : il s'agit de trouver les points entiers et rationnels de la courbe régulière $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Le fait remarquable est que ces courbes peuvent être munis d'une loi de groupe qui géométriquement se définit à la manière de celle sur l'hyperbole. Le théorème de Mordell-Weil dit que pour tout corps $K$, $E(K)$ est un groupe abélien de type fini dont le rang est conjecturalement égal à l'ordre du zéro en $s = 1$ de la fonction $L$ attachée à $E$ ; c'est la version faible de la conjecture de Birch-Swinnerton-Dyer ;
- *travaux de Siegel* : en 1929 Sigel a donné des CNS sur le polynôme $f \in \mathbb{Z}[X, Y]$ pour qu'il possède une infinité de solutions.
- *théorème de Faltings* : soit $C$ une courbe algébrique non singulière de genre $g$ alors :
  - si $g = 0$, il y a soit aucun point rationnel soit une infinité (cf. l'exercice 2.1 ;
  - si $g = 1$, i.e. $C$ est une courbe elliptique, il y a soit un nombre fini de points formant un groupe abélien soit l'ensemble des points rationnels est un groupe abélien de type fini (théorème de Mordell) ;
  - si $g > 1$ il n'y a qu'un nombre fini de points rationnels.

### 2.6 Equation de Thue

Il s'agit d'équations de la forme $F(X, Y) = m$ avec $F(X, Y) \in \mathbb{Z}[X, Y]$ homogène de degré au moins 3. Dès 1909, Thue a montré que ces équations ne possédaient qu'un nombre fini de solution et dans les années 60 Baker parvint à donner une majoration sur la taille des solutions en fonction des coefficients de $F$ et de $m$. Cependant sa majoration était trop large pour être efficace et ce n'est qu'en 1989 que Tzanakis et de Weger ont donnés un algorithme efficace permettant de résoudre ces équations : celui-ci repose sur l'algorithme LLL. La preuve de la finitude du nombre de solutions d'une équation de Thue repose sur le résultat difficile suivant

**Théorème de Thue** *Soit $\alpha \in \mathbb{R}$ un nombre algébrique de degré $d$ ; pour tout $\epsilon > 0$, il existe une constante $C_\epsilon(\alpha) > 0$ telle que pour tout $p/q$ avec $p \wedge q = 1$,*

$$|\alpha - \frac{p}{q}| > \frac{c}{q^{d/2+1+\epsilon}}.$$

**Exercice 2.1.** *Soit $F(x, y) = a_nx^n + a_{n-1}x^{n-1}y + \cdots + a_0y^n \in \mathbb{Z}[x, y]$ un polynôme homogène irréductible de degré $n \geq 3$. Montrez alors que pour tout $m \in \mathbb{Z}$, l'équation diophantienne $F(x, y) = m$ possède un nombre fini de solutions entières.*

## 3 D'autres exemples à traiter au fil de l'avancée du cours

### 3.1 Utilisation d'une extension de corps

Il s'agit de faire de l'arithmétique dans un anneau d'entiers plus gros que $\mathbb{Z}$ dans lequel notre équation se factorise mieux : Le premier exemple évolué a été donné par Kummer sur l'équation de Fermat, précisément pour les $n$ premiers ne divisant pas le nombre de classe de $\mathbb{Q}[e^{2i\pi/n}]$. Pour une illustration de cette technique, nous allons l'appliquer à certaines courbes elliptiques.

**Exercice 3.1.** *Soit $d > 1$ sans facteurs carrés avec $d \equiv 1, 2 \mod 4$, on suppose que le nombre de classes de $\mathbb{Q}(i\sqrt{d})$ n'est pas divisible par 3. Montrez alors $y^2 = x^3 - d$ a une solution entière si et seulement si $d$ est de la forme $3t^2 \pm 1$ auquel ses solutions sont $(t^2 + d, \pm t(t^2 - 3d))$.*

*Remarque :* dans une prochaine feuille on traitera en détail le cas $d = 13$. Les cas $d = 2$ et $d = 4$ sont particulièrement simples puisqu'ils font intervenir respectivement $\mathbb{Z}[i\sqrt{2}]$ et $\mathbb{Z}[i]$ qui sont principaux. Le lecteur pourra s'exercer en prouvant que les solutions entières sont respectivement $(3, \pm 5)$ et $(5, \pm 11)$, $(2, \pm 2)$.

## 3.2 Méthode de Strassmann

On traite l'exemple $x^3 + 6y^3 = \pm 1$ dont on montre que les seules solutions sont $(\pm 1, 0)$. Soit $K = \mathbb{Q}(\theta)$ avec $\theta^3 + 6 = 0$ : on a $r = s = 1$ de sorte que $\mathcal{O}_K$ possède une unique unité fondamentale égale, après calculs, à $1 + 6\theta + 3\theta^2$. L'équation devient

$$N(x - \theta y) = (x - \theta y)(x - j\theta y)(x - j^2\theta y) = \pm 1$$

ou autrement dit $x - y\theta$ est une unité de $\mathcal{O}_k$. Or comme les seules unités d'ordre fini sont $\pm 1$, il existe $k$ tel que

$$x - \theta y = \pm(1 + 6\theta + 3\theta^2)^k = \pm\Big(1 + 3(\theta^2 k + 2\theta k) + 3^2(2\theta^2(k^2 + k)) + 3^3(\cdots) + \cdots\Big).$$

Comme $1, \theta, \theta^2$ est une famille libre de $\mathcal{O}_K$, le coefficient en $\theta^2$ du membre de droite doit être nul ce qui donne une égalité de la forme

$$0 = \pm\Big(3k + 3^2(\cdots) + \cdots\Big)$$

que l'on peut écrire sous la forme $f(k) = 0$ où $f(X) = \sum_{i=1}^{\infty} a_i X$ avec $a_i \in \mathbb{Z}_3$. Comme $v_3(a_1) = 1$ et que pour tout $i > 1$, $v_3(a_i) \geq 2$, le théorème de Strassmann nous dit qu'il existe au plus une solution 3-adique à cette équation. Or comme $k = 0$ est clairement solution, c'est la seule et donc $(x, y) = (\pm 1, 0)$ sont les seules solutions de l'équation $x^3 + 6y^3 = \pm 1$.
*Remarque :* cette méthode à ≪ une variable ≫ a été généralisée à plusieurs variables et donne lieu à la méthode de Skolem, cf. [**?**] §III.2 : jusqu'au année 1980, avant l'apparition de l'algorithme LLL, c'était la méthode principale pour résoudre algorithmiquement les équations diophantiennes.

## 3.3 Principe de Hasse

Une équation diophantienne vérifie le principe de Hasse si l'existence de solutions rationnelles ≪ globales ≫, i.e. sur $\mathbb{Q}$, découle de l'existence de solutions dans $\mathbb{Q}_p$ pour tout $p$ premier ainsi que dans $\mathbb{R}$. L'exemple standard du à Selmer d'une équation diophantienne ne vérifiant pas le principe de Hasse est $3x^3 + 4y^3 + 5z^3 = 0$. Au contraire les formes quadratiques non dégénérées vérifient le principe de Hasse, c'est le fameux théorème de Hasse-Minkowski, cf. [**?**] p.73 : dans le cas particulier des formes ternaires le résultat est du à Legendre, cf. loc. cit. ou [**?**] chapitre 17 §3. Quitte à effectuer un changement de variable, on se ramène à étudier

$$ax^2 + by^2 + cz^2 = 0$$

avec $a, b, c \in \mathbb{Z}$ sans facteurs carrés, premiers entre eux deux à deux. L'existence d'une solution réelle est équivalente au fait que $a, b, c$ ne soient pas tous du même signe ce que nous supposerons désormais. Par ailleurs quitte à multiplier $a$ et $b$ par $c$, et à faire le changement de variable $z' = cz$, on se ramène à étudier $z^2 = ax^2 + by^2$.

**Exercice 3.1.** *Soient $a, b$ des entiers positifs sans facteurs carrés : le but de l'exercice est de montrez que l'équation*

$$ax^2 + by^2 = z^2$$

*possède une solution non triviale si et seulement si les trois conditions suivantes sont vérifiées :*
*(i) $a$ est un carré modulo $b$ ;*
*(ii) $b$ est un carré modulo $a$ ;*
*(iii) $-\frac{ab}{(a \wedge b)^2}$ est un carré modulo $a \wedge b$.*

*(1) Montrez que si l'équation possède une solution non triviale alors les trois conditions de l'énoncé sont vérifiées.*
*(2) Il s'agit désormais de prouver la réciproque.*
*(a) Traitez le cas $a = 1$.*
*(b) Traitez le cas $a = b$.*
*(3) Quitte à échanger les rôles de $x$ et $y$, supposons donc $a > b$. L'idée est alors de construire une nouvelle forme $Ax^2 + by^2 = z^2$ avec $0 < A < a$ satisfaisant les mêmes hypothèses que dans l'énoncé, i.e. $A$ est sans facteurs carrés et les conditions (i), (ii), (iii) sont vérifiées, et telle que si elle possède une solution alors l'équation de l'énoncé aussi. Après un nombre fini d'étapes, en échangeant $A$ et $b$ si $A < b$, on arrive soit à $A = b$ soit à $A = 1$ cas déjà traités.*
*(a) D'après (ii) il existe $T$ et $c$ tels que $c^2 - b = aT = aAm^2$ avec $A$ sans facteurs carrés et $|c| \leq a/2$. Montrez que $0 < A < a$.*
*(b) Prouvez que $AX^2 + bY^2 = Z^2$ vérifie les conditions (i), (ii) et (iii).*
*(c) Montrez que si $AX^2 + bY^2 = Z^2$ possède une solution non triviale alors $(x = AXm, y = cT + Z, z = Zc + bY)$ est une solution non triviale de $ax^2 + by^2 = z^2$.*

On peut alors montrer que $ax^2 + by^2 + cz^2 = 0$ vérifie le principe de Hasse : rappelons que d'après le lemme de Hensel, une équation a une solution dans $\mathbb{Q}_p$ si et seulement si elle a une solution modulo $p^n$ pour tout $n \geq 0$.

**Exercice 3.2.** *Soient $a, b, c$ des entiers non tous de même signe, sans facteurs carrés et premiers entre eux deux à deux. Montrez que si pour tout premier $p$ et tout entier $m$, la congruence*

$$ax^2 + by^2 + cz^2 \equiv 0 \mod p^m$$

*possède une solution $(x, y, z)$ non tous divisibles par $p$ alors $ax^2 + by^2 + cz^2 = 0$ a une solution entière non triviale.*

*Remarque :* dans la situation ci-dessus, la connaissance d'une solution permet de les obtenir toutes ; on renvoie le lecteur au chapitre IV de [**?**]. En illustration on traite un exemple tiré de loc. cit., soit l'équation $x^2 + 11y^2 - 3z^2$ avec la solution $(1, 1, 2)$. On paramètre alors comme suit :

$$(x, y, z) = (1.r, 1.r + p, 2.r + q) \qquad (p, q) \in \mathbb{Q}^2$$

de sorte que l'équation s'écrit

$$(22p - 12q)r = 11p^2 - 3q^2.$$

On élimine alors $r$ pour faire apparaître $x, y, z$ ce qui donne :

$$\begin{array}{l} gx = 11p^2 - 3q^2 \\ gy = 33p^2 - 12pq - 3q^2 \quad (*) \\ gz = 22p^2 + 22pq - 18q^2 \end{array}$$

où on a posé $g = 22p - 12q$. Si on cherche des solutions rationnelles, vu l'homogénéité du système ci-dessus, les solutions sont données par (*) en prenant $g = 1$. En ce qui concerne les solutions entières, quitte à multiplier $p$ et $q$ par le ppcm de leur dénominateur, on peut les supposer entiers et premiers entre eux. Il s'agit alors de trouver les valeurs $g$ telles que l'équation

$$A \begin{pmatrix} p^2 \\ pq \\ q^2 \end{pmatrix} \equiv 0 \mod g \qquad A = \begin{pmatrix} 11 & 0 & -3 \\ 33 & -12 & -3 \\ 22 & 22 & -18 \end{pmatrix}$$

a des solutions. On calcule alors la forme de Smith de $A$ qui est $\mathrm{diag}(66, 2, 1)$ ; $p$ et $q$ étant premiers entre eux, on en déduit $g|66$. Ainsi l'ensemble des solutions entières est la réunion pour $g|66$ des ensembles

$$\{\frac{1}{g}(11p^2 - 3q^2, y = 33p^2 - 12pq - 3q^2, 22p^2 + 22pq - 18q^2) : \ p \wedge q = 1, \ A \begin{pmatrix} p^2 \\ pq \\ q^2 \end{pmatrix} \equiv 0 \mod g\}$$

dont le calcul explicite ne pose pas de problème.

# 4 Solutions

**1.1** Supposons qu'il existe $(x, y, z)$ premiers entre eux satisfaisant $x^n + y^n = z^n$ tels que le maximum des trois degrés soit $D > 0$. On les choisit tels que $D$ soit minimal. Pour $\xi = e^{2i\pi/n}$, on a

$$z^n = (x + y)(x + \xi y)(x + \xi^2 y) \cdots (x + \xi^{n-1} y).$$

Deux facteurs quelconques du produit n'ont pas de diviseur commun puisqu'un tel facteur diviserait $x$ et $y$. Leur produit étant une puissance $n$-ème, ces facteurs sont de la forme $\beta u^n$ avec $\beta \in \mathbb{C}^\times$ qui lui-même est une puissance $n$-ème. Ainsi comme $n - 1 \geq 2$ il existe des polynômes $u, v, w$ tels que

$$x + y = u^n, \quad x + \xi y = v^n, x + \xi^2 y = w^n$$

qui sont donc premiers entre eux. En éliminant $x$ et $y$ de ces équations, on trouve $w^n + \xi u^n = (1 - \xi)v^n$. On pose alors $x' = w$, $y' = \xi^{1/n} u$, $z' = (1 - \xi)^{1/n} v$ de sorte que $(x', y', z')$ constitue une solution de l'équation avec $x', y', z'$ premiers entre eux ($\xi + 1 = 0$ implique $n = 2$) et de degré maximal $D'$ satisfaisant $0 < D' \leq D/n < D$, d'où la contradiction.

**1.2** (1-a) On a $f + g + 1 = 0$ ce qui donne $f' = -g'$ et donc $\frac{b}{a} = \frac{g}{f} = -\frac{f'/f}{g'/g}$.

(1-b) Rappelons que pour $R(x) = \prod_i (x - \rho_i)^{r_i}$, on a $\frac{R'}{R} = \sum_i \frac{r_i}{x - \rho_i}$. Posons

$$a(x) = \prod_i (x - \alpha_i)^{a_i}, \quad b(x) = \prod_j (x - \beta_j)^{b_j}, \quad c(x) = \prod_k (x - \gamma_k)^{c_k},$$

de sorte que

$$\frac{f'}{f} = \sum_i \frac{a_i}{x - \alpha_i} - \sum_k \frac{c_k}{x - \gamma_k}, \qquad \frac{g'}{g} = \sum_j \frac{\beta_j}{x - \beta_j} - \sum_k \frac{c_k}{x - \gamma_k}.$$

Pour $N_0(abc)$ le ppcm des $(x - \alpha_i)$, $(x - \beta_j)$, $(x - \gamma_k)$ qui est donc de degré $n_0(abc)$, on a

$$\frac{b}{a} = -\frac{N_0(abc) f'/f}{N_0(abc) g'/g}$$

où $N_0(abc) f'/f$ et $N_0(abc) g'/g$ sont des polynômes de degré inférieurs ou égaux à $n_0(abc) - 1$. Or comme $a$ et $b$ sont premiers entre eux on en déduit que leur degré est aussi inférieur ou égal à $n_0(abc) - 1$.

(1-c) Pour $c(x)$ la preuve est similaire, ce qui donne le résultat.

(2) Supposons $f^n + g^n = h^n$ de sorte que d'après le théorème précédent on a

$$n \max\{\deg f, \deg g, \deg h\} \leq \deg f + \deg g + \deg h - 1.$$

En ajoutant ces trois inégalités on obtient alors

$$n(\deg f + \deg g + \deg h) \leq 3(\deg f + \deg g + \deg h - 1)$$

et donc $n < 3$.

(3) Notons $a, b, c$ les degrés respectifs de $f, g, h$ ; le théorème précédent donne

$$\alpha a \leq a + b + c - 1 \tag{1}$$
$$\beta b \leq a + b + c - 1 \tag{2}$$
$$\gamma c \leq a + b + c - 1 \tag{3}$$

de sorte que

$$\alpha(a + b + c) \leq \alpha a + \beta b + \gamma c \leq 3(a + b + c) - 3$$

ce qui implique $\alpha < 3$ et donc $\alpha = 2$. La deuxième inégalité donne alors $\beta b + \gamma c \leq 3(b + c) + a - 3$ et comme $\beta \leq \gamma$, de $a \leq b + c - 1$ que l'on obtient à partir de 1, on en déduit

$$\beta(b + c) \leq 4(b + c) - 4$$

et donc $\beta \leq 4$ soit $\beta = 2$ ou 3. Il suffit alors de prouver que pour $\beta = 3$, on a $\gamma \leq 5$. Pour $\beta = 3$, 2 s'écrit $2b \leq a+c-1$ qui ajouté à $a \leq b+c-1$ donne $b \leq 2c-2$ et donc $a \leq 3c-3$ et 3 donne $\gamma c \leq 6c-6$ d'où le résultat.

(4) Soient $x = f/g$ et $y = h/k$ écrits sous forme irréductible une solution de $x^n - y^m = 1$ de sorte que

$$f^m k^n - h^n g^m = g^m k^m.$$

Comme $f$ et $g$ sont premiers entre eux, on obtient que si $g(\alpha) = 0$ alors $k(\alpha) = 0$ ; de même si $k(\alpha) = 0$ alors $g(\alpha) = 0$ de sorte que $g(t) = \prod_i (t - \alpha_i)^{a_i}$ et $k(t) = \prod_i (t - \alpha_i)^{b_i}$ avec $a_i, b_i \geq 1$. Ainsi la multiplicité de $\alpha_i$ comme racine des polynômes $f^m k^n$, $h^n g^m$ et $g^m k^n$ est respectivement égale à $nb_i$, $ma_i$ et $nb_i + ma_i$. Si $nb_i \neq ma_i$ alors la multiplicité de $\alpha_i$ dans $f^m k^n - h^n g^m$ est strictement inférieure à $nb_i + ma_i$ d'où la contradiction. Ainsi $nb_i = ma_i$ i.e. $k^n = g^m$. Après division par $k^n = g^m$, l'équation devient $f^m - h^n = g^m$ qui d'après le corollaire précédent n'a des solutions que pour $\{m, n\} = \{2, 2\}$ ou $\{2, 3\}$. Dans le second cas, on a $k^n = g^m = l^6$ où $l$ est un polynôme alors que l'équation $f^3 - h^2 = l^6$ n'a pas de solutions, d'où le résultat.

**1.3** (1) Si $x = f_1(x)^n + \cdots + f_k(x)^n$ alors pour $h \in \mathbb{C}[x]$, on a $h(x) = f_1^n(h(x)) + \cdots + f_k^n((h(x))$.

(2) Cela résulte simplement de l'identité $(x + \frac{1}{4})^2 - (x - \frac{1}{4})^2 = x$.

(3) Supposons par l'absurde que

$$x = f_1^n(x) + f_2^n(x) = \prod_{r=1}^{n} (f_1 + \zeta^r f_2) \qquad \zeta = e^{2i\pi/n}.$$

Tous les facteurs $f_1 + \zeta^r f_2$, sauf un, sont constants. Pour $n \geq 3$, on dispose d'au moins deux tels facteurs, i.e. il existe $a, b, \alpha, \beta \in \mathbb{C}$ tels que $f_1 + af_2 = \alpha$ et $f_1 + bf_2 = \beta$ avec $a \neq b$. On en déduit alors que $f_1, f_2 \in \mathbb{C}$ d'où la contradiction.

(4) Notons que $\deg(\Delta f) = \deg f - 1$ de sorte que pour $f(x) = x^n$, on a

$$\Delta^{n-1}(x^n) = (x + n - 1)^n + c_1(x + n - 2)^n + \cdots + c_{n-1}x^n = ax + b.$$

On effectue alors le changement de variable $x_1 = ax + b$, on obtient

$$x_1 = f_1^n(x_1) + \cdots + f_n^n(x_1)$$

et donc $k(n) \leq n$.

(5-a) De l'égalité $x = f_1^n(x) + \cdots + f_k^n(x)$, on en déduit que la première colonne de $W_2$ s'obtient à partir de la première colonne de $W_1$ en ajoutant une combinaison linéaire des autres colonnes de $W_1$ de sorte que $W_1 = W_2$. Si $W_2$ s'annule sur un intervalle d'intérieur non vide, un résultat général nous dit qu'il existe un sous-intervalle d'intérieur non vide tel que $x, f_2^n, \cdots, f_k^n$ sont linéairement dépendants ; une telle égalité sur un ensemble infini implique l'égalité des polynômes. Par minimalité de $k$, ce ne peut pas être et donc $W_1$ n'est pas le polynôme nul.

(5-b) La dérivée $r$-ème de $f_i^n$ est divisible par $f_i^{n-r}$ ; ainsi la $i$-ème colonne de $W_1$ est divisible par $f_i^{n-k+1}$ et donc $W_1$ est divisible par $\prod_{i=1}^k f_i^{n-k+1}$. En particulier on a

$$\deg W_1 \geq (n - k + 1) \sum_{i=1}^{k} \deg f_i.$$

(5-c) En multipliant la $j$-ème ligne de $W_2$ par $x^{j-1}$, les termes non nuls de la $i$-ème colonne sont de degré $n \deg f_i$ de sorte que

$$\deg W_2 \leq 1 + n \sum_{i=2}^{k} \deg f_i - 1 - 2 - \cdots - (k-1) = n \sum_{i=2}^{k} \deg f_i - \frac{k(k-1)}{2} + 1.$$

(5-d) On en déduit donc que

$$(n - k + 1) \sum_{i=1}^{k} \deg f_i \leq \deg W_1 = \deg W_2 \leq n \sum_{i=2}^{k} \deg f_i - \frac{k(k-1)}{2} + 1$$

soit $n \deg f_1 \leq (k-1)\sum_{i=1}^k \deg f_i - \frac{k(k1)}{2} + 1$.

(5-e) Si on suppose que $f_1$ est le polynôme de degré maximal alors

$$n \deg f_1 \leq k(k-1)\deg f_1 - \frac{k(k-1)}{2} + 1 \leq k(k-1)\deg f_1$$

car pour $k \geq 3$, on a $-k(k-1) < 0$. Après division par $\deg f_1$, on obtient $n < k(k-1)$ d'où le résultat.

**2.1** (1) l'équation n'a de solutions que si $a \wedge b | c$ auquel cas l'ensemble des solutions est $(x_0 + t\frac{b}{a\wedge b}, y_0 - t\frac{a}{a\wedge b})$ où $(x_0, y_0)$ est une solution particulière que l'on obtient en multipliant par $\frac{c}{a\wedge b}$ une relation de Bezout $au + bv = a \wedge b$ obtenue par l'algorithme d'Euclide étendu.

(2) Via l'isomorphisme $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$, l'équation devient $ny \equiv b \mod (p-1)$ soit à résoudre l'équation suivante dans $\mathbb{Z}$, $ny + \lambda(p-1) = b$, qui possède des solutions si et seulement si $n \wedge (p-1) | b$, i.e. si $b$ appartient au groupe engendré par $n \wedge (p-1)$ et donc si et seulement si l'ordre de $b$ est un diviseur de $\frac{p-1}{n\wedge(p-1)}$. Dans ce cas les solutions sont de la forme $y = y_0 + t\frac{p-1}{n\wedge(p-1)}$ modulo $p-1$ et donc de cardinal celui du sous-groupe de $\mathbb{Z}/(p-1)\mathbb{Z}$ engendré par $\frac{p-1}{n\wedge(p-1)}$ i.e. $n \wedge (p-1)$.

(3) On passe dans $\mathbb{Z}$ soit à résoudre $x + \alpha n = a$ et $x + \beta m = b$ et donc $\alpha n - \beta m = (a-b)$ qui ne possède des solutions que si $n \wedge m$ divise $a - b$.

(4) On écrit $m = ax + by$ et $n = au + bv$ de la façon la plus simple possible, i.e. $0 \leq x, u \leq b-1$, de sorte que l'écriture est unique ; en effet on rappelle que $m = a(x - bt) + b(y + at)$, de sorte qu'il existe un unique $t$ tel que $0 \leq x - bt < b$. L'égalité $m + n = ab - a - b$ donne alors $ab = a(x + u + 1) + b(v + y + 1)$ : $a$ et $b$ étant premier entre eux, "le" théorème de Gauss nous dit que $b$ divise $x + u + 1$. Or on a $1 \leq x + u + 1 \leq 2b - 1$, le seul multiple de $b$ dans cet intervalle est $b$ lui-même, soit $x + u + 1 = b$ et donc $v + y + 1 = 0$. Les nombres $y$ et $v$ étant des entiers, exactement un parmi eux deux est positif ou nul, l'autre étant strictement négatif. En language clair exactement une somme parmi $m$ et $n$ est payable sans rendu de monnaie. En remarquant que 0 est payable, alors $ab - a - b$ n'est pas payable. De même une somme négative n'est pas payable de sorte que si $m > ab - a - b$, la somme $m$ est payable.

**2.2** (1) l'équation n'a de solutions que si $a \wedge \cdots \wedge a_n | b$ auquel cas ses solutions sont $x_i = c_i + \sum_{k=1}^{n-1} d_{i,k} v_k$ où $(c_1, \cdots, c_n)$ est une solution particulière, les $v_i$ sont des paramètres parcourant $\mathbb{Z}$ et les $d_{i,k} \in \mathbb{Z}$ sont .....

(2) Soit $P, Q \in GL_n(\mathbb{Z})$ telles que $A = Q^{-1}DP$ avec $d = \mathrm{diag}(d_1, \cdots, d_r, 0, \cdots, 0) \in \mathbb{M}_{m,n}(\mathbb{Z})$ et où $d_1 | \cdots | d_r \neq 0$. En posant $X' = PX$ et $B' = QB$ le système s'écrit $DX' = B'$ qui se résoud aisément.

**2.3** Le nombre cherché est le coefficient de $z^n$ dans le développement en séries entières de la fraction rationnelle

$$\frac{1}{(1-z)(1-z^2)(1-z^3)} = \Big(\sum_{k=0}^\infty z^k\Big)\Big(\sum_{k=0}^\infty z^{2k}\Big)\Big(\sum_{k=0}^\infty z^{3k}\Big) = \sum_{n=0}^\infty a_n z^n.$$

On décompose alors cette fraction rationnelle en éléments simples ce qui donne :

$$\frac{1}{6(1-z)^3} + \frac{1}{4(1-z)^2} + \frac{17}{72(1-z)} + \frac{1}{8(1+z)} + \frac{1}{9(1-jz)} + \frac{1}{9(1-j^2z)}$$
$$= \sum_{n=0}^\infty \Big(\frac{(n+3)^2}{12} - \frac{7}{72} + \frac{(-1)^n}{8} + \frac{2}{9}\cos\frac{2n\pi}{3}\Big) z^n$$

où on a posé $j = e^{2i\pi/3}$. Le résultat découle alors de la majoration évidente suivante :

$$\Big| -\frac{7}{72} + \frac{(-1)^n}{8} + \frac{2}{9}\cos\frac{2n\pi}{3}\Big| \leq \frac{32}{72} < \frac{1}{2}.$$

**2.4** Le nombre de solutions est égal au coefficient de $z^n$ dans le développement en séries entières de la fraction rationnelle

$$\frac{1}{(1-z)(1-z^2)} + \frac{z}{(1-z^2)(1-z^3)} + \frac{z^2}{(1-z^3)(1-z^4)} + \cdots + \frac{z^k}{(1-z^{k+1})(1-z^{k+2})} + \cdots =$$
$$\frac{1}{z(1-z)}\sum_{k=0}^\infty \Big(\frac{1}{1-z^{k+1}} - \frac{1}{1-z^{k+2}}\Big) = \frac{1}{z(1-z)}\Big(\frac{1}{1-z} - 1\Big) = \sum_{n=0}^\infty (n+1) z^n.$$

**2.5** (1) De l'égalité

$$\sum_{n=0}^{\infty} A_n z^n = \frac{1}{(1-z^{a_1})\cdots(1-z^{a_l})} = \frac{1}{a_1\cdots a_l}\frac{1}{(1-z)^l} + F(z)$$

où $F(z)$ se décompose comme une somme de termes de la forme $\lambda\frac{1}{(1-\omega z)^k}$ où $\lambda \in \mathbb{Q}$, $\omega$ est une racine $a_1\cdots a_l$-ème de l'unité distincte de 1 et, comme $a_1, \cdots, a_l$ n'ont pas de facteurs communs, $k \leq l-1$. Le résultat découle alors de l'écriture

$$\frac{(k-1)!}{(1-\omega z)^k} = \sum_{n=0}^{\infty}(n+k-1)\cdots(n+1)z^n.$$

(2) Comme les $a_i$ sont premiers entre eux deux à deux, on peut écrire $\prod_{i=1}^{l}(1-z^{a_i})$ sous la forme $(1-z)^l Q(z)$ où $Q(z)$ divise $1-z^{a_1\cdots a_l}$. En décomposant en éléments simples le pôle 1, on obtient une égalité du genre

$$\frac{1}{(1-z^{a_1})\cdots(1-z^{a_l})} = R\Big(\frac{1}{1-z}\Big) + \frac{S(z)}{1-z^{a_1\cdots a_l}}$$

où $R(z)$ et $S(z)$ sont des polynômes de degré respectivement égal à $l$ et plus petit que $a_1\cdots a_l$. Le résultat découle alors de l'écriture

$$R\Big(\frac{1}{1-z}\Big) = \sum_{n=0}^{\infty} P(n)z^n, \qquad \frac{S(z)}{1-z^{a_1\cdots a_l}} = \sum_{n=0}^{\infty} Q_n z^n.$$

(3) Soient pour $n < ab$, $ax' + by' = n$ et $ax" + by" = n$ ; on a donc $0 \leq x', x" < b$ et comme l'égalité $a(x'-x") = -b(y'-y")$ avec $a \wedge b = 1$, $-b < x'-x" < b$ est divisible par $b$ et donc nul. En résumé on a $A_n < 2$. Pour $n = ab$, le même raisonnement donne $A_{ab} \leq 2$ et comme $ab + b.0 = ab = a.0 + ba$ on a bien $A_{ab} = 2$.

Comme $a \wedge b = 1$,

$$T(z) = \frac{(1-z^{ab})(1-z)}{(1-z^a)(1-z^b)} = \Phi_1(z) \prod_{\substack{1\neq d_1|a \\ 1\neq d_2|b}} \Phi_{d_1 d_2}(z)$$

est un polynôme de la forme $z^{ab-a-b+1} + \cdots + 1$ avec $T(1) = \frac{ab}{ab} = 1$. On en déduit alors que

$$\frac{T(z)-T(1)}{1-z} = -z^{ab-a-b} + \cdots$$

est aussi un polynôme. On a alors

$$\begin{array}{ll} \sum_{n=0}^{\infty}(A_n - A_{n-ab})z^n & = (1-z^{ab})\sum_{n=0}^{\infty} A_n z^n \\ & = \frac{T(z)}{1-z} \\ & = \frac{T(z)-T(1)}{1-z} + \frac{1}{1-z} \\ & = \cdots - z^{ab-a-b} + \sum_{n=0}^{\infty} z^n \end{array}$$

et donc $A_{ab-a-b} = 0$ et $A_n = A_{n-ab} + 1$ pour tout $n > ab-a-b$. Ainsi on a

$$A_n = A_{n-\lfloor \frac{n}{ab}\rfloor ab} + \lfloor \frac{n}{ab} \rfloor$$

et comme $n - \lfloor \frac{n}{ab} \rfloor ab < n - (\frac{n}{ab}-1)ab = ab$, on en déduit que, comme $A_{n-\lfloor \frac{n}{ab}\rfloor ab} = 0$ ou 1 que $A_n$ est égal à $\lfloor \frac{n}{ab} \rfloor$ ou $\lfloor \frac{n}{ab} \rfloor + 1$.

**2.1** (2) Si $x$ est pair, on a $y^2 \equiv -1 \mod 8$. En écrivant $y$ impair sous la forme $2k+1$, on obtient $y^2 = 1+4k(k+1) \equiv 1 \mod 8$ contradiction. On a $x^3+8 = (x+2)(x^2-2x+4)$ avec $x$ impair de la forme $2k+1$ ; $(x^2-2x+4) = 4k^2+3$. On en déduit donc qu'il existe un $p$ premier divisant $x^2-2x+4$ avec $p \equiv 3 \mod 4$. Or si $p$ premier divise $y^2+1$ alors $p \equiv 1 \mod 4$, d'où la contradiction.

**2.1** (a) On raisonne comme dans l'exercice précédent ; soit $N(a+ib\sqrt{2})=a^2+2b^2$ la norme qui est une fonction multiplicative, et soit $z\in A^\times$ ; on a $zz'=1$ soit $N(z)N(z')=1$ et donc $N(z)=1$, soit $z=\pm 1$.
Pour montrer que $A$ est euclidien, on remarque à nouveau que $z_1/z_2$ peut s'écrire sous la forme $q+e$ avec $q\in A$ et $e\in\mathbb{C}$ de norme strictement plus petite que 1. Ainsi on a $z_1=qz_2+r$, avec $r=z_1-qz_2\in A$ et $N(r)<N(z_2)$.

(b) Si $x$ est pair, on a $y^2\equiv -2 \mod 8$, ce qui ne se peut pas, car les carrés dans $\mathbb{Z}/8\mathbb{Z}$, sont $0,1,4$. On factorise ensuite dans $A$ : $x^3=(y+i\sqrt{2})(y-i\sqrt{2})$ et soit $\delta$ un pgcd de $y+i\sqrt{2}$ et $y-i\sqrt{2}$ ; on a $\delta=(y+i\sqrt{2},(i\sqrt{2})^3)$, or $i\sqrt{2}$ est irréductible car de norme 2, et la seule factorisation de 2 est $1\times 2$, de sorte que $i\sqrt{2}=zz'$ implique que $N(z)=1$ soit $z$ inversible (ou $z'$). Or $i\sqrt{2}$ ne divise pas $y$ car sinon $y^2$ serait pair et donc $y$ pair soit $x$ pair, ce qui n'est pas ; ainsi $\delta=1$. On en déduit donc que $(y\pm i\sqrt{2})$ sont des cubes parfaits : $(y\pm i\sqrt{2})=(a\pm i\sqrt{2})^3$ et $x=a^2+2b^2$. En séparant partie réelle et imaginaire, on trouve alors $y=a^3-6ab^2$ et $1=b(3a^2-2b^2)$ soit $b=\epsilon=\pm 1=3a^2-2$, ce qui donne $b=1$ et $a=\pm 1$ soit $y=\pm 5$ et $x=3$ qui est bien une solution de l'équation.

(c) On a à nouveau $n\in S$ si et seulement si il existe $z\in A$ tel que $n=N(z)$. On étudie à nouveau les irréductibles de $B$ ; $p$ est irréductible si et seulement si $A/(p)$ est intègre, i.e. $X^2+2$ n'a pas de racine dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $-2$ n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, i.e. si et seulement si $p\equiv 5,7 \mod 8$. En raisonnant comme dans l'exercice précédent, on trouve que les irréductibles de $A$, outre les premiers $p\equiv 5,7 \mod 8$, sont les $z\in A$ tels que $N(z)$ est premier. Toujours en suivant la même démarche, on trouve alors que $n\in S$ si et seulement si $v_p(n)$ est pair pour $p\equiv 5,7 \mod 8$.

(d) De la même façon, la détermination de $S$ se fait via l'étude de $A=\mathbb{Z}[\sqrt{2}]$, dont la norme est $a^2-2b^2$, avec le morphisme de corps $c(a+b\sqrt{2})=a-\sqrt{2}b$ de sorte que $N$ est multiplicative. Soit $z\in A^\times$, on a alors $N(z)=\pm 1$. A nouveau $A$ est euclidien pour le stathme $|N|$. On remarque que $-1$ est une norme $-1=1^2-2\times 1^2=N(1+\sqrt{2})$. Si $n$ est un diviseur de $x^2-2y^2$ avec $x,y$ premiers entre eux, alors au signe près $n$ est de la forme $u^2-2v^2$. En effet soit $x+\sqrt{2}y=\pi_1\cdots\pi_r$ une décomposition en produit d'irréductibles ; aucun des $\pi_i$ n'appartient à $\mathbb{Z}$ car $x$ et $y$ sont premiers entre eux, de sorte que comme précédemment les $N(\pi_i)$ sont des premiers de $\mathbb{Z}$ ; on a alors $x^2-2y^2=N(\pi_1)\cdots N(\pi_r)$ et $n$ au signe près, est un produit de certains de ces $N(\pi_i)$ et donc $n$ est de la forme $N(z)=u^2-2v^2$.
L'égalité $-(u^2-2v^2)=N((1+\sqrt{2})(u+v\sqrt{2}))=(u+2v)^2-2(u+v)^2$ permet de négliger le signe $\pm$. Ainsi un premier impair $p$ est de la forme $x^2-2y^2$ si et seulement si 2 est un carré modulo $p$ ce qui est équivalent à $p\equiv\pm \mod 8$.

**2.1** (1) Si $x\equiv y\equiv 0 \mod 2$ alors $z^2\equiv 2 \mod 4$ ce qui est impossible car 0 et 1 sont les seuls carré modulo 4.

(2) On a $(z-x^2)\wedge(z+x^2)=(z-x^2)\wedge 2z=(z-x^2)\wedge 2=2$. On a ainsi $z-x^2=2a^4$ et $z+x^2=2b^4$ avec $a\wedge b=1$ ; le résultat découle alors du fait que comme $2x^2\equiv 2 \mod 4$ exactement un parmi $a$ et $b$ est impair.

(3) On a $x^2=-a^4+4b^4$ ce qui n'est pas car sinon $1\equiv -1 \mod 4$.

(4) on a $z=a^4+4b^4$ et donc, comme $y=2ab\neq 0$, $0<a<z$ ; en éliminant $z$, on a aussi $4b^4=(a^2-x)(a^2+x)$ avec comme $a\wedge x=1$, $(a^2-x)\wedge(a^2+x)=2$. On en déduit comme précédemment $a^2-x=2c^4$ et $a^2+x=2d^4$ de sorte que $a^2=c^4+d^4$. En résumé à partir d'une solution $(x,y,z)$ telle que $z>0$, on en a construit une autre $(c,d,a)$ avec $0<a<z$ et $b=cd\neq 0$. La contradiction découle alors du fait qu'il n'est pas possible de construire une suite infinie d'entiers positifs strictement décroissante.

**2.1** (1) On a $f(z)=2x+3y-i(x+2y)$ de sorte que $F$ est affine avec $F(O)=O$ et de partie linéaire $\vec{F}=\begin{pmatrix}2&3\\1&2\end{pmatrix}$ de déterminant 1, de sorte qu'elle est inversible, conserve les volumes. Ce n'est pas une isométrie puisque ses vecteurs colonnes ne sont pas de norme 1.

Le déterminant étant égal à 1, son inverse est aussi à coefficients dans $\mathbb{Z}$ de sorte que $M\in\mathfrak{S}$ si et seulement si $F(M)\in\mathfrak{S}$. En ce qui concerne $\mathcal{H}$, on a $(2x+3y)^2-3(x+2y)^2=x^2-3y^2=1$.

(2) (i) On calcule $A_1=(2,1)$ et $A_2=(7,4)$. Par récurrence on montre que $A_n\in\mathcal{H}\cap\mathfrak{S}$ en utilisant (1 ii).

(ii) Un point $M(x,y)$ de l'arc $[A_0,A_1]$ de $\mathcal{H}$ est caractérisé par $x^2-3y^2=1$, $1\leq x\leq 2$ et $0\leq y\leq 1$. Si on veut $x,y\in\mathbb{Z}$, on a alors que deux possibilités qui donnent $A_0$ et $A_1$.

(3) (i) On se place dans le repère dont les axes sont les asymptotes de sorte que l'équation est $XY=a$. Il suffit alors d'imposer que $A_0$ soit de coordonnées $(1,1)$. Soient alors $M(a,b)$ et $M'(a',b')$. Supposons dans un premier temps $M\neq N$ et donc $a\neq a'$. La droite $D_{M,N}$ a alors pour équation $\frac{Y-1}{X-1}=\frac{b'-b}{a'-a}$. L'intersection avec $\mathcal{H}$ revient à prendre $Y=1/X$ avec $X\neq 0$ ce qui donne alors $X=aa'$.

Si $M=N$, la tangente en $M$ à $H$ a pour pente $-1/a^2$ ce qui donne $\frac{Y-1}{X-1}=-1/a^2$ et donc avec $XY=1$, $X=a^2$. Ainsi l'application $\phi:\mathcal{H}\to\mathbb{R}^\times$ qui à $M$ associe l'abscisse de $M$ dans le repère $\mathcal{R}$, induit un isomorphisme de $(\mathcal{H},*)$ avec $(\mathbb{R}^\times,\times)$.

**Remarque** : le résultat est valable pour toute hyperbole.

(ii) Si $M\neq A_1$ et $M'\neq A_0$, il s'agit de vérifier que $(A_0M')$et $(MA_1)$ sont parallèles, ce qui revient à montrer que $\begin{vmatrix} 2x+3y-1 & x-2 \\ x+2y & y-1 \end{vmatrix}=3y^2-x^2+1=0$. Si $M=A_1$, la tangente en $A_1$ a pour équation $2x-3y=1$ et a pour vecteur directeur $(3,2)$. Il suffit alors de vérifier que $\begin{vmatrix} 7-1 & 3 \\ 4 & 2 \end{vmatrix}=0$. Si $M'=A_0$ alors $M$ a pour coordonnées $(2,-1)$ et $(A_1M)$ est parallèle à $Oy$ donc à la tangente en $A_0$ à $\mathcal{H}$. Ainsi on a $A_n=A_1*\cdots*A_1$ et donc $X_n=X_1^n$.

(iii) $A_n*A_n$ et $A_{n-1}*A_{n+1}$ sont sur $\mathcal{H}$ et ont même abscisse dans $\mathcal{R}$, ils coincident donc et la construction de $M*N$ donne le résultat. En ce qui concerne l'aire elle est égale à celle de $A_0A_1A_2$ et donc à $\frac{1}{2}\begin{vmatrix} 2-1 & 7-1 \\ 1 & 4 \end{vmatrix}=1$.

(iv) L'arc $[A_n,A_{n+1}]$ de$\mathcal{H}$ est l'ensemble des points $M$ de coordonnées $(X,1/X)$ avec $X_1^{n+1}\leq X\leq X_1^n$ (quitte à échanger les axes, on choisit le repère pour que $X_1<1$). L'application $F$ se traduit par $X\mapsto X_1.X$ et induit donc la bijection de l'énoncé. En particulier d'après (2 ii), on en déduit que $\mathcal{H}\cap\mathfrak{S}$ est formé des $A_n$ et de leurs symétriques par rapport à $Ox$, $Oy$ et $O$.

(4) Les asymptotes de $\mathcal{H}$ ont pour vecteurs directeurs $\vec{u}'=\alpha(\sqrt{3}\vec{u}-\vec{v})$ et $\vec{v}'=\beta(\sqrt{3}\vec{u}+\vec{v})$. Pour que $A_0$ ait pour coordonnées $(1,1$ dans $\mathcal{R}$, on doit avoir $\vec{u}'+\vec{v}'=\vec{u}$ ce qui donne $\alpha=\beta=\frac{1}{2\sqrt{3}}$. On obtient alors $X_1=2-\sqrt{3}$ (et $Y_1=2+\sqrt{3}$). On en déduit alors $X_n=(2-\sqrt{3})^n$ et $Y_n=(2+\sqrt{3})^n$ et donc

$$|x|=\frac{(2+\sqrt{3})^n+(2-\sqrt{3})^n}{2}\qquad |y|=\frac{(2+\sqrt{3})^n-(2-\sqrt{3})^n}{2\sqrt{3}}.$$

**2.2** Evidemment, on se limite à chercher les solutions $x,y\geq 0$.

(i) Pour $N\leq -2$, les seules solutions sont clairement $x=1$ et $y=0$ ; pour $N=-1$, on obtient $(x,y)=(1,0)$ ou $(0,1)$.

(ii) Soit $N=d^2$ ; $x^2-d^2y^2=(x-dy)(x+dy)=1$, soit $x+dy=1=x-dy$, d'où $x=1$ et $y=0$.

(iii) Soit $A=\mathbb{Z}[\sqrt{N}]$ et $N(a+b\sqrt{N})=a^2-Nb^2=(a+b\sqrt{N})(a-b\sqrt{N})$. L'application $N$ est multiplicative, d'où $N((a+b\sqrt{N})(c+d\sqrt{N}))=N(a+b\sqrt{N})N(c+d\sqrt{N})$ ce qui donne l'identité remarquable de l'énoncé.

Avec ces notations $(x,y)$ est solution si et seulement si $N(x+y\sqrt{N})=1$, ainsi si $(x_0,y_0)$ est solution alors $(x_n,y_n)$ tel que $x_n+y_n\sqrt{N}=(x_0+y_0\sqrt{N})^n$, est solution, ce qui donne la relation de récurrence de l'énoncé. On remarque simplement que la suite $(x_n,y_n)$ prend une infinité de valeur car la solution $(x_0,y_0)$ étant non triviale, $x_0\geq 2$ et $y_0\geq 1$ ce qui implique $x_{n+1}>x_n$ et $y_{n+1}>y_n$.

Avec $N=2$ et $(x_0,y_0)=(3,2)$, on obtient les premiers termes de la suite $(x_n,y_n)$ : $(17,12)$, $(99,70)$, $(577,408)$.

(iv) Soient $(x_1,y_1)$ et $(x_2,y_2)$ des solutions positives ; on a alors les équivalences :

$$x_1<x_2\Leftrightarrow x_1^2<x_2^2\Leftrightarrow 1+Ny_1^2<1+Ny_2^2\Leftrightarrow y_1<y_2\Leftrightarrow x_1+y_1\sqrt{N}<x_2+y_2\sqrt{N}$$

On choisit alors la relation d'ordre suivante sur les solutions positives : $(x_1,y_1)\leq(x_2,y_2)$ si et seulement si $x_1\leq x_2$. Parmi les solutions positives non triviales, soit donc $(x_0,y_0)$ la solution minimale dont l'existence découle du fait que $\mathbb{N}$ est discret.

Soit alors $(x,y)$ une solution (positive) et $n\geq 0$ tel que $x_n\leq x<x_{n+1}$ ; on a alors $y_n\leq y<y_{n+1}$ et donc $1\leq\frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}}<x_0+y_0\sqrt{N}$. Or $\frac{x+y\sqrt{N}}{x_n+y_n\sqrt{N}}$ est égal à $X+Y\sqrt{N}$ avec $X=xx_n-Nyy_n$ et $Y=yx_n-xy_n$ avec $X^2-NY^2=1$. En outre, on a $X\geq 0$ car $x\geq y\geq 0$ et $x_n\geq y_n\geq 0$ ; de même $Y\geq 0$ car sinon $X+Y\sqrt{N}=\frac{1}{X+\sqrt{X^2+1}}<1$ ce qui n'est pas. Ainsi $(X,Y)$ est une solution positive et $X+Y\sqrt{N}<x_0+y_0\sqrt{N}$ ce qui contredit la minimalité de $(x_0,y_0)$.

(v) Commençons par montrer l'existence d'une infinité de rationnels $p/q$ tels que $|\sqrt{N}-p/q|<1/q^2$, soit $-1/q<q\sqrt{N}-p<1/q$ et donc soit $p=[q\sqrt{N}]$ soit $p=[q\sqrt{N}]+1$. On raisonne par l'absurde, en supposant la finitude de l'ensemble $E$ de ces rationnels. Soit alors $\epsilon=\min_{p/q\in E}|\sqrt{N}-p/q|$. Comme $\sqrt{N}\notin\mathbb{Q}$, on a $\epsilon>0$. Soit donc $q_0>0$ tel que $1/q_0<\epsilon$, on va montrer qu'il existe $q\leq q_0$ et $p$ tel que $|\sqrt{N}-p/q|<1/qq_0\leq 1/q^2$ ce qui est en contradiction avec le fait que l'on devrait avoir $|\sqrt{N}-p/q|\geq\epsilon$. Considérons donc les $q_0$-tiroirs $[k/q_0,(k+1)/q_0]$

pour $k=0,\cdots,q_0-1$, et les chaussettes $|q\sqrt{N}-[q\sqrt{N}]|$ pour $n=1,\cdots,q_0$. Si une chaussette est dans le premier tiroir, c'est gagné. Plaçons-nous dans la situation contraire et soient $q_1\neq q_2$ deux chaussettes dans le même tiroir, soit $|(q_1-q_2)\sqrt{N}-[q_1\sqrt{N}]+[q_2\sqrt{N}]|<1/q_0$. Ainsi en posant $q=|q_1-q_2|$ et $p=[q_1\sqrt{N}]-[q_2\sqrt{N}]$, on a bien $|a\sqrt{N}-p|<1/q_0$, d'où le résultat.

Des inégalités $-1/q^2<\sqrt{N}-p/q<1/q^2$ avec $p,q>0$, on obtient $-1/q<q\sqrt{N}-p<1/q$, soit $0<p+q\sqrt{N}<1:q+2q\sqrt{N}$ soit $-1-2\sqrt{N}<p^2-Nq^2<1+2\sqrt{N}$. On obtient de la sorte une infinité de couples $(p,q)$ avec $p$ et $q$ premiers entre eux, et $p^2-Nq^2$ appartenant à l'intervalle $[-1-2\sqrt{N},1+2\sqrt{N}]$ dans lequel il y a un nombre fini d'entiers (de tiroirs). Selon le principe des tiroirs, il existe un entier $l$ de l'intervalle précédent tel qu'il existe une infinité de couples $(p,q)$ (les chaussettes) avec $p$ et $q$ premiers entre eux, tels que $p^2-Nq^2=l$. Comme ${}^sqrtN\notin\mathbb{Q}$, $l$ n'est pas nul ; si $l=\pm1$ c'est gagné, sinon les nouveaux tiroirs sont les éléments de $\mathbb{Z}/l\mathbb{Z}$ et on place la chaussette $(p,q)$ dans le tiroir $\bar{p}$. On en déduit donc l'existence d'une infinité de couples $(p,q)$ comme ci-dessus, tels que tous les $p$ ont la même congruence modulo $l$. En envoyant ces chaussettes $(p,q)$ dans le tiroir $\bar{q}$, on obtient finalement l'existence d'un infinité de couples $(p_i,q_i)$ tels que $p_i$ et $q_i$ sont premiers entre eux, $p_i^2-Nq_i^2=l$, tous les $p_i$ ont la même congruence modulo $l$ ; de même que tous les $q_i$.

Soient alors $(p_1,q_1)$ et $(p_2,q_2)$ des éléments distincts de cet ensemble ; on a $p_1^2-Nq_1^2=p_2^2-Nq_2^2=l$ et $p_1\equiv p_2 \mod l$ et $q_1\equiv q_2 \mod l$. Ainsi $p_1q_2-p_2q_1$ est divisible par $l$. De l'égalité $(p_1p_2-Nq_1q_2)^2-N(p_1q_2-p_2q_1)^2=l^2$, on en déduit que $l$ divise $p_1p_2-Nq_1q_2$ et $(\frac{p_1p_2-Nq_1q_2}{l},\frac{p_1q_2-p_2q_2}{l})$ est alors une solution non triviale de l'équation.

**2.1** On écrit l'équation diophantienne sous la forme

$$(\frac{x}{y}-\alpha_1)(\frac{x}{y}-\alpha_2)\cdots(\frac{x}{y}-\alpha_n)=\frac{m}{a_ny^n}.$$

Posons $A=\min_{1\leq i<j\leq n}|\alpha_i-\alpha_j|$. Si $(x,y)$ avec $y\neq0$ est une solution il existe alors au plus un $\alpha_i$ el que $|x/y-\alpha_i|<A/2$ ; $\alpha_i$ étant algébrique de degré $n$, d'après le théorème précédent on a

$$|\frac{x}{y}-\alpha_i|>\frac{C(\epsilon,\alpha_i)}{q^{n/2+1+\epsilon}}$$

et pour $j\neq i$, on a $|x/y-\alpha_j|\geq A/2$. On en déduit alors que

$$\frac{m}{|y|^n}>\frac{T}{|y|^{n/2+1+\epsilon}}$$

avec $T=C(\epsilon,\alpha_i)A^{n-1}/2^{n-1}$ et donc $m>T|y|^{n/2-1-\epsilon}$. On choisit alors $\epsilon$ tel que $n/2-1-\epsilon>0$ ce qui est possible puisque $n\geq3$, de sorte que$|y|$ est bornée. Ainsi le nombre de $y$ est fini, et pour un tel $y$ fixé, il y a au plus $n$ entiers $x$ tels que $(x,y)$ puissent être solutions, d'où le résultat.

**3.1** L'anneau des entiers de $K=\mathbb{Q}(i\sqrt{d})$ est $\mathcal{O}_K=\mathbb{Z}[i\sqrt{d}]$ dont les unités sont $\pm1$, cf. le cours. Soit alors $(x,y)$ une solution de $y^2=x^3-d$. Comme $-d\not\equiv1 \mod 4$, $x$ ne peut pas être pair ; $d$ étant sans facteurs carrés on a aussi $x\wedge d=1$. On écrit

$$x^3=(y+i\sqrt{d})(y-i\sqrt{d}).$$

S'il existait un idéal premier $\mathfrak{P}$ contenant $y\pm i\sqrt{d}$ alors $2i\sqrt{d}\in\mathfrak{P}$ avec $x\in\mathfrak{P}$ de sorte que $N(\mathfrak{P})|4d\wedge x^2=1$ ce qui n'est pas. Ainsi les idéaux $(y+i\sqrt{d})$ et $(y-i\sqrt{d})$ n'ont pas d'idéaux premiers communs dans leur décomposition en produit d'idéaux premiers de sorte qu'il existe un idéal $\mathfrak{A}$ de $\mathcal{O}_K$ tel que

$$(y+i\sqrt{d})=\mathfrak{A}^3,\quad (y-i\sqrt{d})=\bar{\mathfrak{A}}^3.$$

Or comme $3\nmid h$, $\mathfrak{A}^3$ étant principal on en déduit que $\mathfrak{A}$ est principal de sorte qu'il existe $a,b\in\mathbb{Z}$ tels que

$$y+i\sqrt{d}=\pm(a+ib\sqrt{d})^3$$

ce qui donne $1=\pm b(3a^2-db^2)$ et $y=\pm a(a^2-3db^2)$. On en déduit alors $b=\pm1$ et $d=3a^2\pm1$ et donc le résultat.

**3.1** (1) pour (i) et (ii) c'est immédiat et pour (iii), on a $-\frac{a}{a\wedge b}x^2 \equiv \frac{b}{a\wedge b}y^2 \mod a\wedge b$ car $a\wedge b$ divise $z$, et donc $-\frac{ab}{(a\wedge b)^2}$ est un carré modulo $a\wedge b$.

(2-a) Si $a=1$ la proposition est immédiate car $(x,0,x)$ est une solution non triviale et les conditions de l'énoncé sont vérifiées.

(2-b) Si $a=b$ alors d'après (iii), $-1$ est un carré modulo $b$, i.e. il existe $r,s$ tel que $b=r^2+s^2$ ; $x=r$, $y=s$ et $z=r^2+s^2$ est alors une solution non triviale de l'équation.

(3-a) Comme $0\leq c^2=aAm+b$ et $0\leq b<a$, on a $A\geq 0$ et comme $b$ est sans facteurs carrés on a $A\neq 0$ et donc $A>0$. En outre on a $aAm^2<c^2\leq a^2/4$ on a $A\leq Am^2<a/4<a$.

(3-b) (i) : posons $b=b_1d$ et $a=a_1d$ avec $d=a\wedge b$. Comme $a$ et $b$ sont sans facteurs carrés, on a $a_1\wedge d=b_1\wedge d=1$. De $c^2-b_1d=a_1dAm^2$, on tire $d|c$ car $d$ est sans facteurs carrés ; $c=c_1d$ avec $dc_1^2-b_1=a_1Am^2$ i.e. $A(a_1m)^2\equiv -a_1b_1 \mod d$. Or d'après (iii), $-a_1b_1$ est un carré modulo $d$ et comme $m\wedge d=1$, i.e. $m$ est inversible modulo $d$, car sinon $b_1\wedge d\neq 1$, on en déduit que $A$ est un carré modulo $d$. En reprenant le même raisonnement modulo $b_1$ à partir de $c^2\equiv aAm^2 \mod b_1$ et en utilisant que $a$ est un carré modulo $b$ et donc modulo $b_1$, on obtient que $A$ est un carré modulo $b_1$ et donc d'après le lemme chinois car $b_1\wedge d=1$, $A$ est un carré modulo $b$.

(ii) : $b\equiv c^2 \mod A$.

(iii) : posons $A=rA_1$ et $b=rb_2$ avec $r=A\wedge b$. De $c^2-rb_2=arA_1m^2$, on en déduit comme $r$ est sans facteur carré que $r|c$ : $c=rc_2$ et donc $aA_1m^2\equiv -b_2 \mod r$. Comme $a$ est un carré modulo $b$ et donc modulo $r$, on a bien $-A_1b_2$ qui est un carré modulo $r$, en utilisant que comme $m\wedge r=1$, $m$ est inversible modulo $r$.

(3-c) Supposons que $AX^2+bY^2=Z^2$ possède une solution non triviale alors en multipliant $AX^2=Z^2-bY^2$ par $c^2-b=aAm^2$, on obtient

$$a(AXm)^2=(Z^2-bY^2)(c^2-b)=(Zc+bY)^2-b(cY+Z)^2$$

d'après la multiplicativité de l'application $N(x+y\sqrt{b})=x^2-by^2$ de $\mathbb{Q}(\sqrt{b})$, on en déduit que $(x=AXm, y=cT+Z, z=Zc+bY)$ est une solution de $ax^2+by^2=z^2$.

**3.2** On se ramène comme précédemment à l'équation $ax^2+by^2=z^2$ avec $a$ et $b$ positifs sans facteurs carrés. Pour $m=2$ et $p|a$, soit $(x,y,z)$ une solution modulo $p^2$ non triviale modulo $p$. Si $p|y$ alors $p|z$ et comme $p^2$ ne divise pas $a$ alors $p|x$ ce qui n'est pas. On en déduit donc que $b$ est un carré modulo $p$ et comme cela est vrai pour tout $p|a$ et que $a$ est sans facteurs carrés, d'après le lemme chinois, $b$ est un carré modulo $a$. De la même façon $a$ est un carré modulo $b$.

Soit alors $p|d=a\wedge b$ ; on a $p|z$ et si $p$ divisait $x$ ou $y$ alors comme $p^2$ ne divise pas $a$ ou $b$, on en déduit que $p$ divise $x,y,z$, ce qui n'est pas. On a donc $-\frac{a}{d}x^2\equiv\frac{b}{d} \mod p$ et donc $-ab/d^2$ est un carré modulo $p$. Comme précédemment, on conclut, comme $d$ est sans facteurs carrés, que $-ab/d^2$ est un carré modulo $d$. Le résultat découle alors de la proposition précédente.