Équations diophantiennes

Salim Rostam
Complément d'algèbre pour l'agrégation, ENS Rennes

Référence : Combes, Algèbre et géométrie.

Définition 0.1. Une *équation diophantienne*[1] est la donnée d'une fonction $f : \mathbb{R}^m \to \mathbb{R}^n$ pour laquelle on cherche à résoudre l'équation $f(x) = 0$ pour $x \in \mathbb{Z}^m$.

En particulier, ce complément concerne la leçon 126 : Exemples d'équations en arithmétique. Attention, cette leçon concerne également par exemple les équations dans $\mathbb{Z}/n\mathbb{Z}$, que l'on ne mentionnera pas ici.

1 Cas linéaire

1.1 Dimension 1

Proposition 1.1. *Soient $a, b, d \in \mathbb{Z}$. L'équation $ax+by = d$ possède une solution ssi* $\operatorname{pgcd}(a, b) \mid d$. *Dans ce cas, l'ensemble des solutions de l'équation est*

$$S = \{(x_0 - b'k, y_0 + a'k) : k \in \mathbb{Z}\},$$

où $a' \coloneqq \frac{a}{\operatorname{pgcd}(a,b)}$ et $b' \coloneqq \frac{b}{\operatorname{pgcd}(a,b)}$ et (x_0, y_0) est une solution particulière (n'importe laquelle) de $ax + by = d$.

Démonstration. On prouvera la première partie directement dans le cas de n variables. Pour la seconde partie, si $ax + by = d = ax_0 + by_0$ alors $a(x - x_0) = -b(y - y_0)$ donc

$$a'(x - x_0) = -b'(y - y_0).$$

Puisque a' et b' sont premiers entre eux on en déduit que a' divise $y - y_0$, ainsi il existe $k \in \mathbb{Z}$ tel que $ka' = y - y_0$. On trouve donc $y = y_0 + ka'$ et $a'(x - x_0) = -b'ka'$ donc $x - x_0 = -b'k$ donc $x = x_0 - b'k$. □

Pour résoudre entièrement l'équation précédente, il reste donc à trouver une solution particulière à l'équation $ax + by = \operatorname{pgcd}(a, b)$. D'après l'algorithme d'Euclide il existe une suite $r_0 = a_1, r_1 = a_2, \ldots, r_k = 1, r_{k+1} = 0$ avec des divisions euclidiennes

$$(E_{i-1}) : r_{i-1} = b_i r_i + r_{i+1}, \qquad 0 \leq r_{i+1} < r_i,$$

pour tout $i \geq 1$. On *remonte* ensuite l'algorithme, c'est-à-dire on fait en sorte de ne garder que $r_0 = a_1$ et $r_1 = a_2$ dans l'équation initiale $(E_0) : r_0 = b_1 r_1 + r_2$. Plus précisément, pour i allant de 1 à $k - 1$ on réécrit l'équation $r_{i+1} = r_{i-1} - b_i r_i$ en fonction de r_0 et r_1 uniquement.

Exemple 1.2. On cherche une relation de Bézout pour $r_0 = 120$ et $r_1 = 23$.

— on a $120 = 5 \times 23 + 5$ donc $5 = 120 - 5 \times 23$;

1. Diophante d'Alexandrie, entre -100 et 300, parfois surnommé le « père de l'algèbre ».

— on a $23 = 5 \times 4 + 3$ donc $3 = 23 - 4 \times 5 = 23 - 4 \times (120 - 5 \times 23) = -4 \times 120 + 21 \times 23$;
— on a $5 = 1 \times 3 + 2$ donc $2 = 5 - 3 = (120 - 5 \times 23) - (-4 \times 120 + 21 \times 23) = 5 \times 120 - 26 \times 23$;
— on a $3 = 1 \times 2 + 1$ donc $1 = 3 - 2 = (-4 \times 120 + 21 \times 23) - (5 \times 120 - 26 \times 23) = -9 \times 120 + 47 \times 23$.

Si $u_i, v_i \in \mathbb{Z}$ sont tels que $r_i = u_i r_0 + v_i r_1$ alors $u_0 = v_1 = 1$, $u_1 = v_0 = 0$ et $w_{i+1} = w_{i-1} - b_i w_i$ pour $w \in \{u, v\}$ (même relation de récurrence que les r_i). En effet, on a bien $r_i = u_i r_0 + v_i r_1$ pour $i \in \{1, 2\}$, et pour $i \geq 2$ alors

$$\begin{aligned} r_{i+1} &= r_{i-1} - b_i r_i \\ &= (u_{i-1} r_0 + v_{i-1} r_1) - b_i (u_i r_0 + v_i r_1) \\ &= (u_{i-1} - b_i u_i) r_0 + (v_{i-1} - b_i v_i) r_1 \\ &= u_{i+1} r_0 + v_{i+1} r_1. \end{aligned}$$

Une autre façon de trouver une solution particulière est la suivante. Quitte à diviser a et b par leur pgcd, on peut supposer que a et b sont premiers entre eux. Si $\bar{u}$ est l'inverse de a modulo b, on sait donc que b divise $au - 1$ (où $u \in \mathbb{Z}$ est un antécédant de $\bar{u}$ modulo b) et donc si v est tel que $-bv = au - 1$ dans $\mathbb{Z}$ alors c'est gagné. (On fera dans ce sens si $b < a$, et on inversera plutôt b modulo a si $a < b$.)

Exemple 1.3. On cherche une relation de Bézout pour $a = 120$ et $b = 23$. Modulo 23 on a $120 \equiv 5$ car $120 = 5 \times 23 + 5$, et on a $9 \times 5 = 45 \equiv -1 \pmod{23}$ donc $-9 \times 5 \equiv 1 \pmod{23}$. Ainsi -9 est l'inverse de 120 modulo 23 donc 23 divise $120 \times 9 + 1$. On a $120 \times 9 + 1 = (5 \times 23 + 5) \times 9 + 1 = 45 \times 23 + 46 = 47 \times 23$ donc $-9 \times 120 + 47 \times 23 = 1$.

Proposition 1.4. *Soient $a_1, \ldots, a_n \in \mathbb{Z}$ et $d \in \mathbb{Z}$. L'équation diophantienne $\sum_{i=1}^n a_i x_i = d$ possède une solution ssi $\operatorname{pgcd}(a_i)_{1 \leq i \leq n}$ divise d.*

Démonstration. Si le pgcd divise alors par le théorème de Bachet–Bézout il existe des éléments $x'_1, \ldots, x'_s \in \mathbb{Z}$ tels que $\sum_i a_i x'_i = \operatorname{pgcd}(a_i)$ (voir démonstration ci-après), donc $x_i \coloneqq x'_i \times \frac{d}{\operatorname{pgcd}(a_i)}$ convient. Maintenant si l'équation possède une solution alors si δ est un diviseur commun aux a_i alors δ divise d, ainsi le pgcd divise d. On peut aussi dire que par définition on a $\sum_i a_i \mathbb{Z} = \operatorname{pgcd}(a_i)_i \mathbb{Z}$ donc l'équation possède une solution ssi $d \in \operatorname{pgcd}(a_i)_i \mathbb{Z}$ ssi $\operatorname{pgcd}(a_i)_i \mid d$. □

On suppose que $\operatorname{pgcd}(a_i) \mid d$. Pour trouver une solution, on trouve d'aborde une solution de $\operatorname{pgcd}(a_1, a_2) x'_2 + \sum_{i=3}^n a_i x_i = d$. (Remarquons que l'identité suivante est bien vérifiée :

$$\operatorname{pgcd}(a_1, \ldots, a_n) = \operatorname{pgcd}(\operatorname{pgcd}(a_1, a_2), a_3, \ldots, a_n).$$

En effet, un entier d' divise $a_1, \ldots, a_n$ ssi il divise a_1, a_2 et $a_3, \ldots, a_n$ ssi il divise $\operatorname{pgcd}(a_1, a_2)$ et $a_3, \ldots, a_n$.) Finalement, on résout ensuite l'équation $a_1 x_1 + a_2 x_2 = \operatorname{pgcd}(a_1, a_2) x'_2$, qui possède bien une solution puisque $\operatorname{pgcd}(a_1, a_2)$ divise $\operatorname{pgcd}(a_1, a_2) x'_1$! En utilisant le fait qu'on connait l'ensemble des solutions pour le cas $n = 2$, on arrive donc à trouver l'ensemble des solutions dans le cas général.

Exemple 1.5. On cherche à résoudre $2x + 3y + 5z = d$ pour $d \in \mathbb{Z}$ fixé. On a bien $\operatorname{pgcd}(2, 3, 5) = 1 \mid d$ donc l'équation possède des solutions. On a $\operatorname{pgcd}(2, 3) = 1$, donc on résout d'abord $t + 5z = d$. Les solutions sont bien sûr ici les $(t = d - 5z, z)$ pour $z \in \mathbb{Z}$. On résout maintenant $2x + 3y = t$, qui possède des solutions puisque $\operatorname{pgcd}(2, 3) = 1 \mid t$. On a $3 - 2 = 1$ donc $(-t, t)$ est une solution et toute solution est donc de la forme $(-t - 3k, t + 2k)$ pour $k \in \mathbb{Z}$. On conclut que les solutions de l'équation initale sont exactement les $(-d + 5z - 3k, d - 5z + 2k, z)$ pour $z, k \in \mathbb{Z}$.

On trouve donc que l'ensemble des solutions est $d(-1, 1, 0) + (-3, 2, 0)\mathbb{Z} + (5, -5, 1)\mathbb{Z}$. On suppose maintenant $d = 0$. Si l'on essaie de raisonner dès le début avec des bases, on peut dire qu'une base de l'espace des solutions sur $\mathbb{Q}$ est formée par les vecteurs $(-\frac{3}{2}, 1, 0)$ et $(-\frac{5}{2}, 0, 1)$, donc par les vecteurs $a \coloneqq (-3, 2, 0)$ et $b \coloneqq (-5, 0, 2)$. L'ensemble des solutions n'est cependant par $a\mathbb{Z} + b\mathbb{Z}$ puisque le vecteur $(5, -5, 1)$ n'y est pas.

1.2 Cas général

On cherche ici à résoudre l'équation $MX = Y$ d'inconnue $X \in \mathbb{Z}^n$, où $M \in \mathrm{Mat}_{m,n}(\mathbb{Z})$ et $Y \in \mathbb{Z}^m$.

1.2.1 Cas carré inversible

On suppose ici $m = n$.

Proposition 1.6. *Soit A un anneau commutatif unitaire intègre. Une matrice $M \in \mathrm{Mat}_n(A)$ est inversible dans $\mathrm{Mat}_n(A)$ ssi $\det M \in A^\times$.*

Démonstration. Si $MN = I_n$ avec $N \in \mathrm{Mat}_n(A)$ alors $\det(M)\det(N) = 1$ donc $\det(M) \in A^\times$. Réciproquement, dans $\mathrm{GL}_n(\mathrm{Frac}(A))$ on a $M^{-1} = (\det A)^{-1}\mathrm{Com}(M)^\top \in \mathrm{Mat}_n(A)$ donc on en déduit que $M \in \mathrm{GL}_n(A)$. □

Corollaire 1.7. *Une matrice $M \in \mathrm{Mat}_n(\mathbb{Z})$ est inversible dans $\mathrm{Mat}_n(\mathbb{Z})$ ssi $\det M = \pm 1$.*

En particulier, si la matrice M est inversible alors on a simplement $X = M^{-1}Y$.

1.2.2 Cas rectangulaire

Le résultat suivant s'énonce de façon générale pour les matrices à coefficients dans un anneau principal.

Théorème 1.8 (Forme normale de Smith)**.** *Soit $M \in \mathrm{Mat}_{m,n}(\mathbb{Z})$. Il existe un unique entier $s \in \{0, \dots, \min(m,n)\}$ et des uniques entiers strictement positifs $d_1, \dots, d_s \in \mathbb{N}^*$ avec $d_1 \mid \cdots \mid d_s$ tels que*

$$M = P\mathrm{diag}(d_1, \dots, d_s, 0, \dots, 0)Q,$$

pour $P \in \mathrm{GL}_m(\mathbb{Z})$ et $Q \in \mathrm{GL}_n(\mathbb{Z})$. De plus, le coefficient d_1 est le pgcd des coefficients de M.

Remarque 1.9.
- La matrice diagonale est de taille $m \times n$.
- C'est une généralisation de la décomposition donnant le rang d'une matrice.
- Dans un anneau principal, l'unicité est donné par les idéaux (d_i).
- Le produit $d_1 \cdots d_r$ est le pgcd des mineurs de taille r.

La famille $(d_1, \dots, d_s)$ est la famille des *facteurs invariants* de M. L'idée de la preuve repose sur la démarche suivante :
- on permute des lignes et colonnes de M afin de mettre un élément d non nul de valeur absolue minimale de M en haut à gauche ;
- on fait la division euclidenne de chaque élément de la première ligne de M par d, en remplaçant d par le reste (via des opérations sur les colonnes) si ce dernier est non nul ; plus précisément, si $m_{1,j} = qd + r$ alors on fait $C_j \leftarrow C_j - qC_1$, et si $r = 0$ alors on fait de plus $C_1 \leftrightarrow C_j$;
- pareil pour la première colonne.

Notons que lors de la dernière étape, les coefficients de la sous-matrice $\widetilde{M}$ inférieure droite $(m-1) \times (n-1)$ de M ne changent pas puisque la première ligne (excepté le premier coefficient) ne comporte que des 0. Après cette dernière étape, tous les coefficients de la première ligne et colonne de M sont donc nuls, excepté l'élément $\widetilde{d}$ en haut à gauche. Si un élément non nul de $\widetilde{M}$ de divise pas $\widetilde{d}$, on rajoute sa colonne à la première de M et on retourne à l'étape précédente, sinon on recommence l'algorithme dans $\widetilde{M}$.

Exemple 1.10. On suppose ici que $m = 1$. Il s'agit alors d'une équation de la forme $\sum_{i=1}^n a_i x_i = y$ comme traité ci-avant. Le théorème dit qu'on peut se ramener à une équation (facile à résoudre !) de la forme $d_1 x'_1 = \pm y$ où $X' = QX$. Avec la matrice $M = \begin{pmatrix} 2 & 3 & 5 \end{pmatrix}$ de l'Exemple 1.5, on a successivement :

$$\left(\begin{array}{c|ccc|ccc} 1 & 2 & 3 & 5 & 1 & 0 & 0 \\ & & & & 0 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right) \xrightarrow{C_1 \leftarrow C_1 - C_2} \left(\begin{array}{c|ccc|ccc} 1 & -1 & 3 & 5 & 1 & 0 & 0 \\ & & & & -1 & 1 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{C_2 \leftarrow C_2 + 3C_1} \left(\begin{array}{c|ccc|ccc} 1 & -1 & 0 & 5 & 1 & 3 & 0 \\ & & & & -1 & -2 & 0 \\ & & & & 0 & 0 & 1 \end{array}\right)$$

$$\xrightarrow{C_3 \leftarrow C_3 + 5C_1} \left(\begin{array}{c|ccc|ccc} 1 & -1 & 0 & 0 & 1 & 3 & 5 \\ & & & & -1 & -2 & -5 \\ & & & & 0 & 0 & 1 \end{array}\right),$$

donc avec $Q = \begin{pmatrix} 1 & 3 & 5 \\ -1 & -2 & -5 \\ 0 & 0 & 1 \end{pmatrix}$ on a $MQ = \begin{pmatrix} -1 & 0 & 0 \end{pmatrix}$. Remarquons qu'on a bien $Q \in \mathrm{GL}_3(\mathbb{Z})$ puisque $\det Q = \begin{vmatrix} 1 & 3 \\ -1 & -2 \end{vmatrix} = -2 + 3 = 1$. Ainsi, si $2x + 3y + 5z = d$ alors $MX = (d)$ avec $X = \begin{pmatrix} x & y & z \end{pmatrix}^\top$ donc avec $X' = Q^{-1}X$ on a $DX' = (d)$ avec $D = \begin{pmatrix} -1 & 0 & 0 \end{pmatrix}$. Les solutions sont donc $x' = -d$ et $y', z' \in \mathbb{Z}$ donc on trouve

$$X = QX' = \begin{pmatrix} 1 & 3 & 5 \\ -1 & -2 & -5 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} -d \\ y' \\ z' \end{pmatrix} = \begin{pmatrix} -d + 3y' + 5z' \\ d - 2y' - 5z' \\ z' \end{pmatrix},$$

donc $x = -d + 3y' + 5z'$, $y = d - 2y' - 5z'$ et $z = z'$. (On retrouve bien les solutions de l'Exemple 1.5, où le z est notre z' et le k est notre $-y'$.)

Si $M = PDQ$ avec P, D, Q comme dans le théorème, alors résoudre $MX = Y$ revient à résoudre l'équation $DX' = P^{-1}Y$ d'inconnue $X' \in \mathbb{Z}^n$. La matrice D étant diagonale, c'est très facile. On obtient ensuite les solutions du système initiale puisque $X = Q^{-1}X'$.

2 Sommes de carrés

Soit $q \in \mathbb{Z}[X_1, \ldots, X_N]$ un polynôme. Une question naturelle est la suivante : peut-on décrire l'ensemble des entiers représentés par q, c'est-à-dire

$$\{n \in \mathbb{Z} : n = q(x_1, \ldots, x_n) \text{ pour } x_1, \ldots, x_n \in \mathbb{Z}\}?$$

C'est une question très générale et difficile. On peut choisir de se restreindre au cas où q est homogène de degré 2, c'est-à-dire une forme quadratique. Les deux résultats que nous allons présenter ici concernent en fait le cas où q est une somme de carrés (avec $N = 2$ et $N = 4$).

2.1 Théorème des deux carrés

(Perrin, §II.6.) Le but est de déterminer l'ensemble

$$\Sigma := \{n \in \mathbb{N} : n = x^2 + y^2, x, y \in \mathbb{N}\}.$$

Lemme 2.1. *Si $n \in \Sigma$ alors $n \neq 3 \pmod 4$.*

Démonstration. Pour $x \in \mathbb{N}$ on a $x^2 = 0, 1 \pmod 4$ donc $x^2 + y^2 = 0, 1, 2 \pmod 4$. □

Pour la suite, on introduit l'anneau $\mathbb{Z}[i] \subseteq \mathbb{C}$ des *entiers de Gauss*. Notamment, on a l'identité

$$x^2 + y^2 = (x + iy)(x - iy). \tag{2.2}$$

L'anneau $\mathbb{Z}[i]$ est un anneau euclidien, pour le stathme donné par $N : z \mapsto |z|^2$, ses inversibles sont ses éléments de norme 1 à savoir $\{\pm 1, \pm i\}$. En outre, l'ensemble des nombres sommes de deux carrés est stable par multiplication, c'est pourquoi il suffit de se restreindre au cas premier.

Lemme 2.3. *Pour p premier on a $p \in \Sigma \iff p$ n'est pas irréductible dans $\mathbb{Z}[i]$.*

Démonstration. Si $p \in \Sigma$ alors $p = a^2 + b^2 = (a + ib)(a - ib)$. Puisque $a, b \neq 0$ (car p n'est pas un carré car premier) on en déduit que $a + ib, a - ib \notin \{\pm 1, \pm i\} = \mathbb{Z}[i]^\times$ donc p n'est pas irréductible. Réciproquement, si p n'est pas irréductible dans $\mathbb{Z}[i]$ alors $p = zz'$ avec $z, z' \in \mathbb{Z}[i]$ et $N(z), N(z') \neq 1$ donc $N(p) = p^2 = N(z)N(z')$ donc $N(z) = N(z') = p$ donc $p \in \mathbb{Z}[i]$. □

Théorème 2.4. *Soit p un nombre premier. L'équation $x^2 + y^2 = p$ possède des solutions si et seulement si $p = 2$ ou $p = 1 \pmod 4$.*

Démonstration. Le théorème est vrai si $p = 2 = 1^2 + 1^2$. On suppose maintenant $p > 2$. D'après les Lemmes 2.1 et 2.3, il suffit de montrer que si $p = 1 \pmod 4$ alors p n'est pas irréductible dans $\mathbb{Z}[i]$. Si $p = 1 \pmod 4$ alors -1 est un carré modulo p (pour rappel, ssi $(-1)^{\frac{p-1}{2}} = 1$, cf. complément sur la cyclotomie), donc il existe $a \in \mathbb{Z}$ tel que $-1 = a^2 \pmod p$ donc $p \mid a^2 + 1 = (a+i)(a-i)$. Ainsi, on a $(a+i)(a-i) \in (p)$ et donc l'idéal (p) n'est pas premier puisque $a \pm i \notin (p)$ puisque $p \nmid 1$. Puisque $\mathbb{Z}[i]$ est euclidien, il est factoriel donc irréductible = premier [2]. Ainsi, l'élément p n'est pas irréductible dans $\mathbb{Z}[i]$ et c'est ce qu'on voulait. □

Corollaire 2.5. *Soit $n \geq 2$, que l'on écrit $\prod_p p^{v_p(n)}$. L'équation $x^2 + y^2 = n$ possède des solutions si et seulement si $v_p(n)$ est pair pour tout $p \equiv 3 \pmod 4$.*

Démonstration. Il suffit de se rappeler que Σ est stable par multiplication, que tout carré est dans Σ et que si $p = 3 \pmod 4$ alors p est irréductible dans $\mathbb{Z}[i]$ donc premier car $\mathbb{Z}[i]$ est factoriel donc si $n = x^2 + y^2$ alors p divise $(x - iy)(x + iy)$ donc p divise $x + iy$ (par exemple), donc p divise x et y donc $p^2 \mid n$ donc $\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ et on récurre. □

2.2 Théorème des quatre carrés

Théorème 2.6 (Conjecture de Bachet, Théorème des Quatre Carrés de Lagrange)**.** *Tout entier positif peut s'écrire comme la somme de quatre carrés d'entiers.*

Démonstration. Voir la preuve de Wikipédia sur l'article en anglais correspondant. C'est un calcul. □

La preuve repose sur une descente infinie et sur l'*identité des quatre carrés d'Euler*, qui dit qu'une produit de deux sommes de quatre carrés est encore une somme de quatre carrés. Cette dernière identité peut facilement se montrer via le corps des quaternions $\mathbb{H}$, en rappelant que $N(q) = q\overline{q} = x^2 + y^2 + z^2 + t^2$ et $N(qq') = N(q)N(q')$ (voir par exemple le Perrin pour ce point). En particulier, cette identité montre qu'il suffit encore une fois de montrer le théorème pour les nombres premiers, c'est-à-dire, que tout nombre premier s'écrit comme la somme de quatre carrés d'entiers.

2. De façon général, un élément premier est toujours irréductible. Si l'anneau est factoriel, la réciproque est vraie.

3 Équation de Fermat

On regarde l'équation $(F_n) : x^n + y^n = z^n$ pour $n \geq 1$. Les triplets $(x, 0, x)$ et $(0, x, x)$, et $(x, -x, 0)$ si n est impair, sont tous solution : ce sont les solutions vérifiant $xyz = 0$, on parle de solution *triviale*. On cherche alors les solutions non triviales de (F_n), c'est-à-dire avec x, y, z tous non nuls. On a bien sûr le théorème suivant, totalement hors de portée du programme de l'agrégation.

Théorème 3.1 (Fermat [3], Wiles [4] 1994)**.** *Si $n \geq 3$ alors (F_n) ne possède pas de solution non triviale.*

3.1 Résolution totale

Proposition 3.2 (Cas $n = 1$)**.** *L'équation (F_1) possède une infinité de solutions non triviales, qui sont toutes de la forme $(x, y, x + y)$ pour $x, y \in \mathbb{Z}$.*

Proposition 3.3 (Cas $n = 2$)**.** *L'équation (F_2) possède une infinité de solutions non triviales, qui sont toutes de la forme*

$$(x, y, z) \text{ ou } (y, x, z) = \big(k(b^2 - a^2), 2kba, k(b^2 + a^2)\big),$$

pour $k, a, b \in \mathbb{Z}$. De plus, avec $x, y, z > 0$ cette paramétrisation est bijective si on prend $k, a, b > 0$ et $a < b$ premiers entre eux.

Démonstration. On vérifie que les triplets donnés sont bien solution. Réciproquement, soit maintenant (x, y, z) une solution non triviale. On peut bien sûr supposer que $x, y, z > 0$ puisqu'on a des carrés. De plus, quitte à diviser par leur pgcd (que l'on peut noter k), on peut supposer que x, y et z sont premiers entre eux (dans leur ensemble). En réalité, si p est un diviseur premier de x et y alors p divise $x^2 + y^2 = z^2$ donc p divise z : ainsi nécessairement x, y et z sont deux à deux premiers entre eux. En particulier, un seul des trois est pair ; on suppose dans la suite, quitte à permuter x et y si jamais x est pair, que x est impair.

Si $z = 0$ alors $x = y = 0$, et si $y = 0$ alors $x = \pm z = \pm 1$ (d'après l'hypothèse premiers entre eux). En particulier, on a $z \neq 0$ donc le point $(\frac{x}{z}, \frac{y}{z})$ est un point du cercle unité. On peut donc écrire $\frac{x}{z} = \cos\theta$ et $\frac{y}{z} = \sin\theta$ avec $\theta \in]-\pi, \pi[$ ($\theta \neq \pi$ puisque $y \neq 0$). Avec $t = \tan\frac{\theta}{2}$, on a donc

$$\frac{x}{z} = \frac{1 - t^2}{1 + t^2}, \qquad \frac{y}{z} = \frac{2t}{1 + t^2}.$$

On va maintenant montrer que t est rationnel. En effet, on a

$$\frac{x}{y} = \frac{1 - t^2}{2t} = \frac{t^{-1} - t}{2} \in \mathbb{Q}, \qquad \frac{z}{y} = \frac{1 + t^2}{2t} = \frac{t^{-1} + t}{2} \in \mathbb{Q},$$

donc

$$\frac{z}{y} - \frac{x}{y} = \frac{t^{-1} + t}{2} - \frac{t^{-1} - t}{2} = t \in \mathbb{Q},$$

Ainsi, en écrivant $t = \frac{a}{b}$ avec $\text{pgcd}(a, b) = 1$, on a d'une part $(1 + t^2)x = (1 - t^2)z$ donc $(b^2 + a^2)x = (b^2 - a^2)z$. Puisque x et z sont premiers entre eux, on en déduit que z divise $a^2 + b^2$ donc on peut écrire

$$mz = a^2 + b^2,$$

3. Pierre de Fermat, début 1600 - 1665 (France).
4. Andrew Wiles, 1953 Cambridge.

et on trouve donc $mxz = (b^2 - a^2)z$ donc

$$mx = b^2 - a^2. \tag{\dagger}$$

On a d'autre part $(1+t^2)y = 2tz$ donc $(b^2+a^2)y = 2abz$ donc, puisque $mz = a^2 + b^2$, on trouve

$$my = 2ab.$$

Maintenant, puisque a et b sont premiers entre eux on sait que $\operatorname{pgcd}(a^2+b^2, a^2-b^2) \leq 2$. En effet, si d est un facteur commun alors d divise leur somme $2a^2$ et leur différence $2b^2$. Si d est impair alors d divise a^2 et b^2, qui sont premiers entre eux (pas de facteur premier commun) donc $d = 1$, et si d est pair alors $\frac{d}{2}$ divise a^2 et b^2 donc $\frac{d}{2} = 1$.

On sait que m est un facteur commun à a^2+b^2 et a^2-b^2 donc $m = 1$ ou 2. Si $m = 1$ c'est gagné, et si $m = 2$ alors nécessairement a et b sont de même parité et donc nécessairement impairs. Mais alors a et b sont $\equiv \pm 1 \pmod 4$, ainsi $a^2 \equiv b^2 \equiv 1 \pmod 4$ donc (†) donne $2x = b^2 - a^2 \equiv 0 \pmod 4$ donc x est pair, ce qui est exclu. □

Remarque 3.4. On a vu que, si on prend x, y, z premiers entre eux dans leur ensemble (donc après avoir divisé par le pgcd), seul un d'entre eux est pair. Nécessairement c'est soit x soit y (celui qui correspond au terme $2ba$), en particulier z est impair.

Remarque 3.5. Un triplet $(x, y, z) \in \mathbb{N}^3$ solution de (F_2) est appelé *triplet pythagoricien*. Un triplet est pythagoricien si et seulement s'ils forment les côtés d'un triangle rectangle ; la Proposition 3.3 liste donc les triangles rectangles à côtés entiers.

Remarque 3.6. On a paramétré un point (a, b) du cercle unité via la tangente de l'angle moitié. Une autre façon d'obtenir cette paramétrisation est de regarder l'intersection du cercle unité avec la droite $y = t(1+x)$ pour un $t \in \mathbb{R}$. On peut par exemple réutiliser cette méthode pour étudier l'équation

$$x^3 + y^3 = xyz$$

(cf. Combes, §12.7 Exercice 2). À savoir, en coupant la courbe $\mathcal{C}$ d'équation $X^3 + Y^3 = XY$ (c'est le folium de Descartes) par les droites d'équation $Y = tX$ on obtient le paramétrage rationnel $X = \frac{t}{t^3+1}, Y = \frac{t^2}{t^3+1}$ des points $(X, Y) \in (\mathcal{C} \setminus \{(0,0)\}) \cap \mathbb{Q}^2$. En effet si $t \in \mathbb{Q}$ alors $X, Y \in \mathbb{Q}$, et réciproquement si $X, Y \in \mathbb{Q}$ (avec $X \neq 0$) alors $t = \frac{Y}{X} \in \mathbb{Q}$. Si $t = \frac{a}{b}$ avec $\operatorname{pgcd}(a, b) = 1$ alors on obtient notamment $x = ab^2, y = a^2 b$ et $z = a^3 + b^3$.

Corollaire 3.7. *L'équation (F_4) n'a pas de solution non triviale (i.e. avec au moins une des variable nulle). Plus précisément, l'équation $x^4 + y^4 = z^2$ ne possède pas de solution avec $xyz \neq 0$.*

Démonstration. (Voir Combes, §12.7 Proposition 2.) Si $x^4 + y^4 = z^4$ alors $x^4 + y^4 = (z^2)^2$. Il suffit donc de montrer que $x^4 + y^4 = z^2$ ne possède pas de solution non triviale. On choisit une solution (x, y, z) avec z minimal. Le triplet (x^2, y^2, z) est pythagoricien donc on peut écrire $x^2 = b^2 - a^2$, $y^2 = 2ba$ et $z = b^2 + a^2$ (après avoir divisé par le pgcd). On a alors $x^2 + a^2 = b^2$, on réapplique la Proposition 3.3 et on arrive à trouver un triplet (α, β, γ) avec $\alpha^4 + \beta^4 = \gamma^2$ avec $0 < \gamma < z$, ce qui est une contradiction. □

La démonstration précédente utilise le *principe de descente infinie* de Fermat.

Remarque 3.8. De la même façon, on montre que $x^4 - y^4 = z^2$ ne possède pas de solution non triviale. Cela signifie qu'il n'existe aucun triangle rectangle à côtés entiers d'aire carrée. En effet, si c'était le cas on aurait $a^2 + b^2 = c^2$ et $\frac{ab}{2} = d^2$, donc $ab = 2d^2$ et

$$\begin{aligned}\left(a^2 - b^2\right)^2 &= \left(a^2 + b^2\right)^2 - 4a^2b^2 \\ &= c^4 - (2d)^4.\end{aligned}$$

Ainsi la solution obtenue de $x^4 - y^4 = z^2$ est triviale donc $xyz = 0$. Puisque $a, b > 0$ on a $x, y \neq 0$, donc $z = 0$ et $a = b$, mais alors $2a^2 = c^2$ ce qui est impossible puisque 2 n'est pas un carré dans $\mathbb{Z}$.

Remarque 3.9. Euler avait conjecturé que l'équation $x^4 + y^4 + z^4 = t^4$ ne possède pas de solution non triviale. En 1988, Noam D. Elkies a démontré qu'il y a en fait une infinité de solutions non triviales... la plus petite (trouvée par Roger Frye) étant $(95800, 217519, 414560, 422481)$!

On a l'étape de réduction importante suivante, qui justifie le fait que l'on s'intéressera à la suite au cas n premier uniquement.

Lemme 3.10. *Soit $n \geq 2$. Si l'équation (F_n) possède une solution alors l'équation (F_d) possède une solution pour tout diviseur d de n.*

Démonstration. Soient x, y, z tels que (x, y, z) est solution de (F_n). Si $n = dm$ alors on a $(x^m)^d + (y^m)^d = (z^m)^d$ donc (x^m, y^m, z^m) est solution de (F_d). □

Remarque 3.11. Attention, la réciproque n'est pas vraie, cf. le cas $n = 4$ et $d = 2$.

Ainsi, on s'intéressera maintenant à l'équation (F_p) pour p premier impair (le cas $p = 2$ ayant déjà été traité). Le reste de cette sous-section est consacrée au cas $p = 3$, et est tirée de la note de S. Vinatier « Le théorème de Fermat pour p régulier, $p \nmid xyz$ » accessible en ligne (ou le corrigé du sujet de MG19 !).

Proposition 3.12. *L'équation (F_3) ne possède pas de solution (x, y, z) vérifiant $xyz \neq 0 \pmod 3$.*

Démonstration. Remarquons que pour $x \in \mathbb{Z}$ alors x^3 est congru à 0 ou ± 1 modulo 9. En effet, modulo 9 on a :

$$0^3 \equiv 0, \qquad 1^3 \equiv 1,$$
$$2^3 \equiv 8 \equiv -1, \qquad 3^3 \equiv 9 \cdot 3 \equiv 0,$$
$$4^3 \equiv 16 \cdot 4 \equiv -2 \cdot 4 \equiv -8 \equiv 1.$$

En particulier, on a $x^3 \equiv 0 \pmod 9$ ssi $x \equiv 0 \pmod 3$. Ainsi, si $xyz \neq 0 \pmod 3$ alors $x, y, z \neq 0 \pmod 3$ donc $x^3, y^3, z^3 \equiv \pm 1 \pmod 9$. Mais alors $x^3 + y^3 \equiv 0, \pm 2 \neq \pm 1 \pmod 9$ donc $x^3 + y^3 \neq z^3 \pmod 9$. □

On note $j \coloneqq e^{\frac{2i\pi}{3}} \in \mathbb{C}$. L'élément j vérifie $j^2 + j + 1 = 0$ et on considère l'anneau $\mathbb{Z}[j] \subseteq \mathbb{C}$ (anneau des *entiers d'Eisenstein*). Les propriétés que l'on va énoncer ont déjà été rencontrées en §2.1.

Lemme 3.13. *Soit $N : \mathbb{C} \to \mathbb{R}_+$ donnée par $N = |\cdot|^2$.*

(i) Pour tout $z \in \mathbb{Z}[j]$, il existe un unique couple $(x, y) \in \mathbb{Z}$ tel que $z = x + jy$.

(ii) Pour tous $x, y \in \mathbb{Q}$ on a $|x + jy|^2 = x^2 - xy + y^2$. En particulier, l'application N restreinte à $\mathbb{Z}[j]$ ne prend que des valeurs dans $\mathbb{N}$.

(iii) L'application N est un stathme euclidien sur l'anneau $\mathbb{Z}[j]$, en particulier $\mathbb{Z}[j]$ est factoriel.

(iv) Pour $u \in \mathbb{Z}[j]$ on a $u \in \mathbb{Z}[j]^\times \iff N(u) = 1$. En particulier, on a $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

(v) Si $x \in \mathbb{Z}[j]$ est tel que $N(x)$ est un nombre premier alors x est irréductible.

Démonstration. (i) L'existence découle de la relation $j^2 = -1 - j$, et l'unicité du fait que $X^2 + X + 1$ est le polynôme minimal de j sur $\mathbb{Q}$ (ou, plus simplement, que $j \notin \mathbb{Q}$ puisque $\sin \frac{2\pi}{3} \neq 0$ puisque $\frac{2}{3} \notin \mathbb{Z}$).

(*ii*) En rappelant que $\bar{j} = j^2$, on a :

$$\begin{aligned} |x+jy|^2 &= (x+jy)(x+j^2y) \\ &= x^2 + (j+j^2)xy + j^3y^2 \\ &= x^2 - xy + y^2. \end{aligned}$$

On conclut puisqu'alors $|x+jy|^2 = (x-y)^2 + xy$.

(*iii*) Soient $x, y \in \mathbb{Z}[j]$ avec $y \neq 0$. Écrivons $\frac{x}{y} = \frac{x\overline{y}}{N(y)^2} = p + qj$ avec $p, q \in \mathbb{Q}$. On peut trouver $a, b \in \mathbb{Z}$ tels que $|p-a| \leq \frac{1}{2}$ et $|q-b| \leq \frac{1}{2}$. On trouve alors par le point précédent que

$$\begin{aligned} \left|(a+bj) - (p+qj)\right|^2 &= \left|(a-p) + j(b-q)\right|^2 \\ &= (a-p)^2 - (a-p)(b-q) + (b-q)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} \\ &\leq \frac{3}{4}. \end{aligned}$$

On considère maintenant $z \coloneqq a+jb \in \mathbb{Z}[j]$, qui approxime $p+qj = \frac{x}{y}$. On a $x = zy + (x-zy)$ et

$$\begin{aligned} N(x-zy) &= N(y)N\left(\frac{x}{y} - z\right) \\ &= N(y)N\big(p+qj-(a+bj)\big) \\ &\leq \frac{3}{4}N(y) \\ &< N(y), \end{aligned}$$

ce qui conclut la preuve.

(*iv*) Puisque $uv = 1$ alors $N(uv) = N(u)N(v) = 1$ donc $N(u) = 1$ puisque $N(u), N(v) \in \mathbb{N}$. Réciproquement, si $N(u) = 1$ alors $u\overline{u} = N(u) = 1$ donc $u \in \mathbb{Z}[j]^\times$ puisque $\overline{u} \in \mathbb{Z}[j]$ (puisque $\bar{j} = j^2 = -1 - j$). Finalement, par le deuxième point, si $u = a + jb \in \mathbb{Z}[j]^\times$ alors $a^2 - ab + b^2 = 1$, ce qui se réécrit $\left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = 1$, en particulier $|b| \leq 1$. Si $b = 0$ alors $u = a = \pm 1$, et sinon $b = \pm 1$ et $a - \frac{b}{2} = \frac{\epsilon}{2}$ avec $\epsilon \in \{-1, 1\}$ donc $a = \frac{b+\epsilon}{2} \in \{0, b\}$. Ainsi, on trouve $u = \pm(1+j) = \mp j^2$ ce qui conclut.

(*v*) Si $x = yz$ pour $y, z \in \mathbb{Z}[j]$ alors $N(x) = N(y)N(z)$ donc $N(y)$ ou $N(z) = 1$. Ainsi y ou z est inversible par le point précédent donc x est irréductible.

□

Remarque 3.14. Attention, la réciproque du dernier point n'est pas vérifiée : par exemple, l'élément 5 est irréductible dans $\mathbb{Z}[j]$ (à vérifier !) mais $N(5) = 25$ n'est pas premier.

Lemme 3.15. *Soit $\lambda \coloneqq 1 - j \in \mathbb{Z}[j]$.*

(*i*) *On a $N(\lambda) = -j^2\lambda^2 = 3$, en particulier λ est un élément premier de $\mathbb{Z}[j]$ et $\lambda \mid 3$.*

(*ii*) *On a $\lambda \nmid 2$.*

(*iii*) *Pour tout $x \in \mathbb{Z}[j]$ on a $x = 0, \pm 1 \pmod{\lambda}$. De plus, si $\epsilon = \pm 1$ alors*

$$x = \epsilon \pmod{\lambda} \iff x^3 = \epsilon \pmod{\lambda^3} \iff x^3 = \epsilon \pmod{\lambda^4}.$$

(*iv*) *Si $u \in \mathbb{Z}[j]^\times$ est tel que $u = 1 \pmod{\lambda^3}$ alors $u = 1$.*

Démonstration. (*i*) On a $N(\lambda) = 1^2 - (-1) + (-1)^2 = 3$ donc λ est irréductible par le Lemme 3.13, donc premier puisque $\mathbb{Z}[j]$ est factoriel. De plus, on a $\overline{\lambda} = 1 - j^2 = -j^2(-j + 1) = -j^2\lambda$ donc on conclut puisque $N(\lambda) = \lambda\overline{\lambda}$.

(*ii*) Si $2 = \alpha\lambda$ alors $N(2) = N(\alpha)N(\lambda)$ donc $4 = N(\alpha)3$ ce qui est impossible puisque $N(\alpha) \in \mathbb{N}$.

(*iii*) Soit $x = a + jb \in \mathbb{Z}[j]$. On a $x = a + b + (j-1)b = a + b - \lambda b$ et $a + b = 0, \pm 1 \pmod 3$ donc on a également $a + b = 0, \pm 1 \pmod \lambda$ puisque $\lambda \mid 3$. Finalement, on a bien $x = 0, \pm 1 \pmod \lambda$.

Si $x^3 = \epsilon \pmod{\lambda^4}$ alors $x^3 \pmod \epsilon \pmod{\lambda^3}$ donc $x \neq 0 \pmod \lambda$. Si $x = -\epsilon \pmod \lambda$ alors $x^3 = -\epsilon = \epsilon \pmod{\lambda^3}$ donc $2 = 0 \pmod \lambda^3$ donc $\lambda \mid 2$, ce qui est impossible par le point précédent. On en conclut donc que $x = \epsilon \pmod \lambda$.

Supposons maintenant maintenant $x = 1 \pmod \lambda$ et montrons $x^3 = 1 \pmod{\lambda^4}$ (ce qui impliquera également $x^3 = 1 \pmod{\lambda^3}$). On a $x = 1 + t\lambda$ avec $t \in \mathbb{Z}[j]$ et

$$\begin{aligned} x^3 - 1 &= (x-1)(x-j)(x-j^2) \\ &= t\lambda(x - 1 + 1 - j)(x - 1 + 1 - j^2) \\ &= t\lambda(t\lambda + \lambda)(t\lambda - j^2\lambda) \\ &= t(t+1)(t-j^2)\lambda^3. \end{aligned}$$

Si $t = 0$ ou $-1 \pmod \lambda$ on conclut, et sinon par le début du point on a nécessairement $t = 1 \pmod \lambda$ donc $t - j^2 = 1 - j^2 = -j^2\lambda = 0 \pmod \lambda$. Le cas $x = -1 \pmod \lambda$ s'en déduit.

(*iv*) Par le Lemme 3.13, il suffit de voir que si $u \in \{-1, \pm j, \pm j^2\}$ alors $u \neq 1 \pmod{\lambda^3}$. On a :
— si $u = -1$, alors $u - 1 = -2$;
— si $u = -j$ alors $u - 1 = -j - 1 = \lambda - 2$;
— si $u = -j^2$ alors $u - 1 = -j^2 - 1 = j^2(-j - 1) = j^2(\lambda - 2)$;
donc puisque $\lambda \nmid 2$ (et $-1, j^2 \in \mathbb{Z}[j]^\times$) on en déduit $\lambda \nmid u - 1$ donc $\lambda^3 \nmid u - 1$. On a finalement :
— si $u = j$ alors $u - 1 = j - 1 = \lambda$;
— si $u = j^2$ alors $u - 1 = j^2 - 1 = j^2(1 - j) = -j^2\lambda$;
donc on conclut puisque $\lambda^3 \nmid \lambda$ (puisque $\lambda = 1 - j$ n'est pas inversible par le Lemme 3.13). □

Puisque $\mathbb{Z}[j]$ est factoriel et que λ est un élément premier, on peut considérer la valuation λ-adique $v_\lambda : \mathbb{Z}[j] \setminus \{0\} \to \mathbb{N}$.

Théorème 3.16. *Soit $u \in \mathbb{Z}[j]^\times$. L'équation $x^3 + y^3 = uz^3$ ne possède pas de solution pour $x, y, z \in \mathbb{Z}[j]$ tous non nuls, premiers entre eux (dans $\mathbb{Z}[j]$) et vérifiant $0 = v_\lambda(x) = v_\lambda(y) < v_\lambda(z)$.*

Démonstration. On suppose qu'il existe un tel triplet et on en choisit un tel que $v_\lambda(z) \geq 1$ est minimal (pour tous les $u \in \mathbb{Z}[j]^\times$), en particulier, on a $\lambda \mid z$. Remarquons que les éléments x et y sont premiers entre eux dans $\mathbb{Z}[j]$ car si π est un diviseur premier commun alors π divise $x^3 + y^3 = uz^3$ donc π divise uz^3 donc π divise z^3 (car u inversible) donc π divise z (car π premier) donc π divise $\operatorname{pgcd}(x, y, z) = 1$.

Puisque $\lambda \nmid x, y$ on en déduit par le Lemme 3.15 que $x^3, y^3 = \pm 1 \pmod{\lambda^3}$. Puisque $z^3 = 0 \pmod{\lambda^3}$ on en déduit que nécessairement $x^3 = -y^3 = 1 \pmod{\lambda^3}$, quitte à permuter x et y. En effet, on ne peut pas avoir $x^3 = y^3 \pmod{\lambda^3}$ puisque $2 \neq 0 \pmod{\lambda^3}$ par le Lemme 3.15. Ainsi par le Lemme 3.15 on a $x^3 = -y^3 = 1 \pmod{\lambda^4}$, et donc $z^3 = 1 - 1 = 0 \pmod{\lambda^4}$ donc $3v_\lambda(z) = v_\lambda(z^3) \geq 4$ donc

$$v_\lambda(z) \geq 2,$$

en particulier $v_\lambda(z^3) \geq 6$.

De façon analogue à (2.2), on a

$$z^3 = x^3 + y^3 = \prod_{k=0}^{2} (x + j^k y), \tag{3.17}$$

(cf. racines de $X^3 + y^3$). Ainsi, il existe $k \in \{0, 1, 2\}$ tel que $v_\lambda(x + j^k y) \geq 2$. Quitte à remplacer y par $j^{-k}y$ on peut supposer que $k = 0$, ainsi $\lambda^2 \mid x + y$. On a alors

$$x + jy = x + y + (j - 1)y = x + y - \lambda y,$$

donc $\lambda \mid x + jy$ et donc $\lambda \mid \mathrm{pgcd}(x + y, x + jy)$. On a en fait égalité : si $d \in \mathbb{Z}[j]$ divise $x + y$ et $x + jy$ alors d divise la différence λy et de plus d divise $j(x + y) - (x + jy) = (-1 + j)x = -\lambda x$. Ainsi, l'élément d divise $\mathrm{pgcd}(\lambda y, \lambda x) = \lambda \mathrm{pgcd}(y, x) = \lambda$ puisque x et y sont premiers entre eux. Finalement, puisque $\lambda^2 \mid x + y$ on en déduit que $\lambda^2 \nmid x + jy$ (car λ n'est pas inversible dans $\mathbb{Z}[j]$) et donc $v_\lambda(x + jy) = 1$. On montre de même que $\mathrm{pgcd}(x + y, x + j^2 y) = \mathrm{pgcd}(x + jy, x + j^2 y) = \lambda$ et $v_\lambda(x + j^2 y) = 1$, et par (3.17) on en déduit que $v_\lambda(x + y) = v_\lambda(z^3) - 2 \geq 4$.

Encore par (3.17), on a

$$\prod_{k=0}^{2} \frac{x + j^k y}{\lambda} = \left(\frac{z}{\lambda}\right)^3,$$

de plus par ce qui précède les facteurs de gauche sont deux à deux premiers entre eux donc on en déduit que ce sont des cubes, à des inversibles près. Pour chaque k on peut donc écrire $x + j^k y = u_k \alpha_k^3 \lambda$ pour $\alpha_k \in \mathbb{Z}[j]$ premiers entre eux et $u_k \in \mathbb{Z}[j]^\times$. De plus $\alpha_k \neq 0$ puisque $z \neq 0$, et par (3.17) et ce qui précède on sait que

$$3v_\lambda(\alpha_0) + 1 = v_\lambda(x + y) = v_\lambda(z^3) - 2 = 3v_\lambda(z) - 2,$$

donc $v_\lambda(\alpha_0) = v_\lambda(z) - 1 \geq 1$. Puisque $\lambda^2 \nmid x + j^k y$ pour $k \in \{1, 2\}$ on en déduit $v_\lambda(\alpha_k) = 0$ pour $k \in \{1, 2\}$. On a finalement

$$\sum_{k=0}^{2} j^k \left(x + j^k y\right) = x \sum_{k=0}^{2} j^k + y \sum_{k=0}^{2} j^{2k} = 0,$$

donc on obtient $\sum_{k=0}^{2} j^k u_k \alpha_k^3 \lambda = 0$ et

$$j \frac{u_0}{u_2} \alpha_0^3 + j^2 \frac{u_1}{u_2} \alpha_1^3 + \alpha_2^3 = 0. \tag{3.18}$$

En passant modulo λ^3 dans (3.18) on obtient, en rappelant le Lemme 3.15,

$$j^2 \frac{u_1}{u_2} \pm 1 = 0 \pmod{\lambda^3},$$

donc $\epsilon \coloneqq j^2 \frac{u_1}{u_2} \in \mathbb{Z}[j]^\times$ ne peut être que ∓ 1 par le Lemme 3.13.(*iv*) et le Lemme 3.15.(*iv*). Puisque $(-1)^3 = -1$, l'équation (3.18) devient :

$$(\epsilon \alpha_1)^3 + \alpha_2^3 = -\frac{j u_0}{u_2} \alpha_0^3,$$

avec $\epsilon = \mp 1$. Finalement, les α_k sont non nuls, premiers entre eux, $v_\lambda(\alpha_k) = 0$ pour $k \in \{1, 2\}$ et $1 \leq v_\lambda(\alpha_0) < v_\lambda(z)$. Puisque $-\frac{j u_2}{u_0} \in \mathbb{Z}[j]^\times$ on obtient donc une contradiction avec le fait que $v_\lambda(z)$ est minimal. □

Encore une fois, le raisonnement précédent est analogue à une descente infinie.

Corollaire 3.19. *L'équation (F_3) ne possède pas de solution (entière) non triviale.*

Démonstration. Soient $x, y, z \in \mathbb{Z}$ tous non nuls solution de (F_3). Quitte à diviser par leur pgcd, on peut supposer que x, y, z sont premiers entre eux dans $\mathbb{Z}$. Remarquons qu'alors x, y et z sont également premiers entre eux dans $\mathbb{Z}[j]$, puisque $\mathbb{Z}$ est principal (et on peut donc trouver une relation de Bézout dans $\mathbb{Z}$ pour x, y, z, ainsi si $\delta \in \mathbb{Z}[j]$ divise x, y et z alors δ divise 1). Par la Proposition 3.12, on sait que $3 \mid xyz$, donc puisque $x^3 + y^3 + (-z)^3 = 0$ on peut tout à fait supposer que $3 \mid z$, en particulier $\lambda \mid z$ (puisque $\lambda \mid 3$, cf. Lemme 3.15). Si maintenant $\lambda \mid x$ alors $\lambda \mid y^3$ donc $\lambda \mid y$, puisque λ est premier dans $\mathbb{Z}[i]$ par le Lemme 3.15, ce qui contredit le fait que x, y, z sont premiers entre eux dans $\mathbb{Z}[j]$, donc on en déduit que $\lambda \nmid x, y$. Mais par le Théorème 3.16 c'est impossible ! □

3.2 Résolution partielle

On va maintenant donner des résultats partiels : on va regarder les solutions (x, y, z) de (F_p), pour p premier, vérifiant $xyz \neq 0 \pmod p$ (on rappelle qu'il est naturel de regarder les cas p premiers par le Lemme 3.10).

Proposition 3.20. *L'équation (F_5) ne possède pas de solution (x, y, z) vérifiant $xyz \neq 0 \pmod 5$.*

Démonstration. La même méthode que dans le cas $p = 3$ s'applique (cf. Proposition 3.12). Modulo 25, on a

$$0^5 \equiv 0, \qquad 1^5 \equiv 1,$$
$$2^5 \equiv 32 \equiv 7, \qquad 3^5 \equiv 9 \times 27 \equiv 9 \times 2 \equiv 18 \equiv -7,$$
$$4^5 \equiv 16^2 \times 4 \equiv 9^2 \times 4 \equiv 81 \times 4 \equiv 6 \times 4 \equiv 25 \equiv -1,$$

et pour tout $k \in \mathbb{Z}$ on a $(k+5)^5 = k^5 + 5 \times (\cdot) = k^5 \pmod 5$. On en déduit que $\{x^5 : x \in \mathbb{Z}/25\mathbb{Z}\} = \{0, \pm 1, \pm 7\}$ avec $x^5 = 0 \pmod{25} \iff x = 0 \pmod 5$. Ainsi, si $xyz \neq 0 \pmod 5$ alors x^5, y^5, z^5 sont ± 1 ou ± 7 et l'égalité $x^5 + y^5 = z^5$ est impossible. □

Remarque 3.21. La méthode ne s'applique plus pour $p = 7$. Par exemple, on a $1^7 + 2^7 = 3^7 \pmod{49}$ (c'est $1 + 30 = 31$) et en fait ça marche pour n'importe quelle puissance de 7.

On a en fait les deux résultats plus généraux suivants.

Théorème 3.22 (Théorème de Sophie Germain [5])**.** *Soit p un nombre premier impair tel que $2p+1$ soit également premier. L'équation (F_p) ne possède pas de solution avec $xyz \neq 0 \pmod p$.*

Démonstration. Oraux X-ENS algèbre. C'est du calcul. □

Remarque 3.23.
- L'énoncé est en fait un cas particulier du théorème.
- Un nombre premier comme dans le théorème s'appelle un *nombre premier de Sophie Germain*. Les premiers nombres premiers de Sophie Germain impairs sont $3, 5, 11, 23, 29$ (notamment, on a vu que le théorème est vrai pour 3 et 5). On ne sait pas s'il y en a une infinité.

Théorème 3.24 (Kummer [6])**.** *Soit p un entier impair et $\zeta \in \mu_p^\times(\mathbb{C})$. On suppose que l'hypothèse suivante est vérifiée :*

5. Sophie Germain, 1776 (Paris) - 1831 (Paris).
6. Ernst Eduard Kummer, 1810–1893, allemand.

pour tout idéal $I \subseteq \mathbb{Z}[\zeta]$, si I^p est principal alors est principal.

Alors (F_p) ne possède pas de solution avec $xyz \neq 0 \pmod p$.

Démonstration. LMLP, 131 développements pour l'oral, développement 24. Voir également la note de P. Caldero « Étude de l'équation de Fermat pour les premiers réguliers » et celle de Vinatier précédente. □

Remarque 3.25.
— On a $I^p = \{\sum_{i=1}^p a_1 \cdots a_p : a_i \in I\}$. On ne sais pas si l'hypothèse est vérifiée pour un nombre infini de premiers p. On parle de premier *régulier* ; les premiers nombres premiers qui ne sont *pas* réguliers sont 37, 59, 67.
— La preuve fait un peu penser à celle du Théorème 3.16, la différence majeure étant ici que si $\mathbb{Z}[\zeta]$ n'est plus factoriel. À la place, on utilise le fait que tout idéal de $\mathbb{Z}[\zeta]$ peut se décomposer en un produit d'idéaux premiers.
— La démonstration est la porte grande ouverte aux questions relatives aux corps de nombres, vous êtes prévenus !

Finalement, concluons cette partie avec le résultat suivant.

Théorème 3.26 (Grand théorème de Fermat modulaire)**.** *Il existe un entier q_n tel que pour tout entier premier $p > q_n$, l'équation (F_n) admette une solution (x, y, z) dans $\mathbb{Z}/p\mathbb{Z}$ avec $xyz \neq 0$.*

Remarque 3.27.
— La démonstration est principalement combinatoire et pas vraiment difficile, mais elle fait intervenir des outils inhabituels pour nous (c'est une application de la *théorie de Ramsay*). Elle peut cependant passer en développement (voir par exemple le pdf de Pierre Le Barbenchon).
— Pour p premier alors $x^p + y^p = (x+y)^p$ dans $\mathbb{Z}/p\mathbb{Z}$. En particulier, pour trouver un triplet avec $x^p + y^p = z^p$ dans $\mathbb{Z}/p\mathbb{Z}$ il suffit de prendre $x + y = z$ (avec $xyz \neq 0 \pmod p$).

4 Autres équations

On présente ici quelques exemples divers d'équations diophantiennes, avec des méthodes de résolution diverses.

Proposition 4.1 (L'unique entier entre un carré et un cube, 131DPA)**.** *L'équation $x^2 + 2 = y^3$ pour $x, y \in \mathbb{N}$ possède une unique solution, qui est $x = 5$ et $y = 3$.*

Démonstration. Utilise la factorialité de $\mathbb{Z}[i\sqrt{2}]$. □

Le résultat précédent montre que 26 est l'unique entier entre un carré et un cube, ici $25 = 5^2$ et $27 = 3^3$.

Proposition 4.2. *La seule solution de l'équation $a^b = b^a$ pour $1 \leq a < b$ entiers est $a = 2$ et $b = 4$.*

Démonstration. Voir Oraux X-ENS 4.2. On peut étudier la fonction $x \mapsto \frac{\ln x}{x}$ ou alors raisonner avec $\operatorname{pgcd}(a, b)$. □

Proposition 4.3. *Soit $N \geq 1$ et $k \geq 2$. L'équation $n(n+1)(n+2) = N^k$ n'a pas de solution pour $n \in \mathbb{N}$.*

Démonstration. Oraux X-ENS 4.22 *Un produit de trois entiers consécutifs [...]*. C'est un petit calcul. □

Proposition 4.4. *Soit $n, \alpha \in \mathbb{N}$ avec $\alpha > n \geq 2$. L'équation*

$$x_1^2 + \cdots + x_n^2 = \alpha x_1 \cdots x_n,$$

n'a pas de solution entière autre que $x_1 = \cdots = x_n = 0$.

Démonstration. Oraux X-ENS algèbre, 4.38 *Une équation diophantienne.* On regarde les racines du polynôme $X^2 - \alpha x_1 \cdots x_{n-1} X + \sum_{i=1}^{n-1} x_i^2$ et on conclut par une descente infinie. □