Une équation diophantienne

Daniel PERRIN

Le point de départ de ce texte est une question posée dans le bulletin APM numéro 537, question 537-3 : *résoudre en nombres entiers les équations* $x^2+y^2=31z^2$ *et* $x^2+y^2=29z^2$. On résout d'abord ici ces deux équations de manière élémentaire (c'est-à-dire en restant dans l'anneau des entiers). On s'intéresse ensuite à l'équation plus générale $x^2+y^2=kz^2$ avec $k \in \mathbf{N}^*$, que l'on notera (E_k) et que l'on résout en utilisant les entiers de Gauss [1].

1 Une solution élémentaire

1.1 Quelques remarques

1.1 *Remarques.* 1) Il revient au même de résoudre (E_k) dans $\mathbf{N}$ ou dans $\mathbf{Z}$. En effet, si l'on a une solution x, y, z dans $\mathbf{N}$ on trouve les solutions $\pm x, \pm y, \pm z$ dans $\mathbf{Z}$ et inversement, si l'on a une solution x, y, z dans $\mathbf{Z}$, on a la solution $|x|, |y|, |z|$ dans $\mathbf{N}$.

2) Si x, y, z est une solution dans $\mathbf{N}$ ou $\mathbf{Z}$ et si d divise x, y, z, $\frac{x}{d}, \frac{y}{d}, \frac{z}{d}$ est une autre solution. Inversement, si x, y, z est solution, il en est de même de dx, dy, dz avec $d \in \mathbf{N}$. On est ainsi ramené à étudier les solutions **primitives**, c'est-à-dire avec x, y, z premiers entre eux.

1.2 L'équation $x^2+y^2=31z^2$

1.2 Proposition. *L'équation* $x^2+y^2=31z^2$ *n'a pas de solution distincte de* $(0,0,0)$ *dans* $\mathbf{Z}^3$.

Démonstration. Il suffit de montrer que l'équation n'a pas de solution primitive non nulle. On utilise les congruences. Modulo 4 les entiers sont congrus à $0, 1, 2$ ou -1 donc leurs carrés à 0 ou 1. Une somme de deux carrés est donc congrue à $0, 1$ ou 2. Supposons que l'on a une solution primitive x, y, z de $x^2+y^2=31z^2$. Si z est impair, donc z^2 congru à 1 modulo 4, comme 31 est congru à -1, $31z^2=x^2+y^2$ aussi et c'est absurde. Si z est pair, z^2 est congru à 0 modulo 4, donc aussi la somme x^2+y^2 et cela impose que x et y sont tous deux pairs, ce qui est absurde car la solution est supposée primitive.

1. Une approche "élémentaire" de l'équation générale est possible, mais hormis dans le cas où k est premier, cette méthode est plutôt plus compliquée que celle qui consiste à utiliser le passage par les complexes, voir remarque 4.7.

1.3 L'équation $x^2 + y^2 = 29z^2$

1.3.1 Des solutions

Comme on a $29 = 2^2 + 5^2$, l'équation admet les solutions évidentes $x = 2$, $y = 5$, $z = 1$ et $x = 5$, $y = 2$, $z = 1$. De plus, on a aussitôt d'autres solutions grâce à l'identité de Lagrange [2] :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

En effet, si $u, \pm v, z$ est une solution de l'équation (de Pythagore) $u^2+v^2 = z^2$, en écrivant $(2^2 + 5^2)(u^2 + v^2)$ avec Lagrange, on en déduit que $x = 2u - 5v$, $y = 5u+2v$, z et $x = 2u+5v$, $y = 5u-2v$, z sont solutions de $x^2+y^2 = 29z^2$. Comme on connaît une infinité de solutions de l'équation $u^2 + v^2 = z^2$ (par exemple $u = a^2 - b^2$, $v = 2ab$, $z = a^2 + b^2$ avec $a, b \in \mathbf{Z}$, voir 2.7 ci-dessous), on obtient une infinité de solutions de l'équation donnée.

1.3.2 Toutes les solutions ?

En fait, on obtient ainsi toutes les solutions de l'équation :

1.3 Théorème. *Toutes les solutions dans $\mathbf{Z}^3$ de l'équation $x^2 + y^2 = 29z^2$ sont de l'une des formes $x = 2u - 5v$, $y = 5u + 2v$, z ou $x = 2u + 5v$, $y = -5u+2v$, z, où u, v, z est une solution dans $\mathbf{Z}^3$ de l'équation $u^2+v^2 = z^2$.*

Si z est premier avec 29, et si u, v, z est une solution primitive de $u^2+v^2 = z^2$, les solutions ci-dessus sont primitives.

Démonstration. Soit x, y, z une solution de l'équation, que l'on peut supposer primitive. On note d'abord que $(2x + 5y)(2y + 5x) = 29xy + 10(x^2 + y^2)$ est multiple de 29 et, de même pour $(2x - 5y)(2y - 5x)$. Comme 29 est premier, il divise l'un des facteurs de chaque produit et il ne peut diviser à la fois $2x + 5y$ et $2x - 5y$, sinon il diviserait $4x$ et $10y$, donc x et y, de sorte que 29^2 diviserait $29z^2$, donc 29 diviserait aussi z, contrairement à l'hypothèse que la solution est primitive.

Il y a donc deux cas : soit 29 divise $2x+5y$ et $2y-5x$, soit il divise $2x-5y$ et $2y + 5x$. Dans le premier cas, on pose $2x + 5y = 29u$, $2y - 5x = 29v$ avec $u, v \in \mathbf{Z}$, dont on déduit $x = 2u - 5v$, $y = 5u + 2v$. En élevant au carré on trouve $29^2(u^2 + v^2) = 29(x^2 + y^2)$, d'où $u^2 + v^2 = z^2$ comme annoncé.

Le second cas est analogue : on a $29u = 2x - 5y$, $29v = 5x + 2y$ d'où $x = 2u + 5v$ et $y = 2v - 5u$ avec $u^2 + v^2 = z^2$.

2. Que l'on comprend mieux à partir de la formule $(a+ib)(c+id) = (ac-bd)+i(ad+bc)$ dans $\mathbf{Z}[i]$ en passant aux normes, voir plus loin.

Montrons que les solutions données sont primitives sous les hypothèses de l'énoncé. Traitons le premier cas, l'autre est analogue. Si x, y, z n'est pas primitive, il existe p premier qui divise $2u - 5v$, $5u + 2v$ et z. Il divise alors $2(2u - 5v) + 5(5u + 2v) = 29u$ et, comme z est premier avec 29, p divise u. Mais p divise aussi $5(2u - 5v) - 2(5u + 2v) = -29v$, donc il divise v. Cela contredit le fait que u, v, z est une solution primitive de $u^2 + v^2 = z^2$.

1.4 *Remarques.* 1) Les deux expressions donnant x, y sont nécessaires. Ainsi, on vérifie que la solution $x = 5$, $y = 2$, qui est du type $x = 2u + 5v$, $y = -5u + 2v$ avec $u = 0$, $v = 1$ ne s'écrit pas sous la forme $x = 2u - 5v$, $y = 5u + 2v$.

2) Si z est multiple de 29, on a $u^2 + v^2 \equiv 0 \pmod{29}$, donc $4u^2 \equiv -4v^2 \equiv 25v^2$, autrement dit, 29 divise $4u^2 - 25v^2 = (2u - 5v)(2u + 5v)$. On voit que 29 divise $2u - 5v$ ou $2u - 5v$ (et pas les deux sinon la solution u, v, z ne serait pas primitive). Cela signifie que l'une des solutions x, y, z est primitive et l'autre non.

1.3.3 Description des solutions

1.5 Théorème. *Les solutions primitives de l'équation $x^2 + y^2 = 29z^2$ dans $\mathbf{N}$ sont de la forme suivante : $x = |2(a^2 - b^2) - 10\epsilon ab|$, $y = |5\epsilon(a^2 - b^2) + 4ab|$, $z = a^2 + b^2$ avec $\epsilon = \pm 1$, $a, b \in \mathbf{N}^*$, premiers entre eux, non tous deux impairs et vérifiant $a > b$, ou les mêmes formules en échangeant x et y.*

Si z est premier avec 29, les solutions ci-dessus sont primitives.

Démonstration. On choisit une solution primitive de l'équation de Pythagore $u^2 + v^2 = z^2$. À l'échange près de u et v, qui revient échanger x et y, on a : $u = a^2 - b^2$, $v = 2ab$, $z = a^2 + b^2$ (voir 2.7 ci-dessous). On calcule $x = 2u - 5\epsilon v$ et $y = 5\epsilon u + 2v$ avec $\epsilon = \pm 1$ et on trouve les expressions annoncées au signe près. Les valeurs absolues donnent alors les solutions dans $\mathbf{N}$.

1.6 *Exemple.* Dans tous les exemples on confond les solutions (x, y, z) et (y, x, z).

Avec $a = 1$, $b = 0$, qui donne la solution $(1, 0, 1)$ de l'équation de Pythagore, on trouve la solution évidente $x = 2, y = 5$, $z = 1$ de l'équation.

Avec $a = 2$, $b = 1$, qui donne la solution $(3, 4, 5)$ de Pythagore, on a deux possibilités :

- $x = 14$, $y = 23$, $z = 5$: $14^2 + 23^2 = 196 + 529 = 725 = 29 \times 5^2$,
- $x = 26$, $y = 7$, $z = 5$: $26^2 + 7^2 = 676 + 49 = 725$.

Avec $a = 3$ et $b = 2$ on a la solution $5, 12, 13$ de Pythagore et on trouve les solutions $50, 49, 13$ et $70, 1, 13$.

1.7 *Remarque.* Avec $a = 5$ et $b = 2$, on a $u = 21$, $v = 20$ et $z = 29$. On est dans le cas où k et z ne sont pas premiers entre eux. On obtient les solutions $(142, 65, 29)$ et $(58, 145, 29)$. La première est primitive, mais pas la deuxième.

2 Quelques rappels

2.1 Rappels sur $\mathbf{Z}[i]$ et les sommes de deux carrés

La présence de $x^2 + y^2$ dans le premier membre de (E_k) indique que la question est liée au problème des sommes de deux carrés, qui se résout par exemple en utilisant l'anneau $\mathbf{Z}[i]$ des entiers de Gauss[3], c'est-à-dire l'ensemble des nombres complexes $a + ib$ avec $a, b \in \mathbf{Z}$, l'idée étant de factoriser $x^2 + y^2 = (x + iy)(x - iy)$ dans cet anneau. On renvoie le lecteur à [1] pour toutes précisions. Voici les résultats dont nous aurons besoin :

2.1 Théorème. *L'anneau $\mathbf{Z}[i]$ est principal. Ses éléments inversibles sont $1, -1, i, -i$. Ses éléments irréductibles sont associés[4] aux suivants :*

1) les nombres premiers de $\mathbf{N}$ congrus à -1 modulo 4,

2) les éléments $\alpha + \beta i$ et $\alpha - \beta i$ avec $\alpha^2 + \beta^2$ premier de $\mathbf{N}$, congru à 1 modulo 4 et $0 < \alpha < \beta$,

3) l'élément $1 + i$.

Tout élément w non nul de $\mathbf{Z}[i]$ s'écrit de manière unique[5] sous la forme $w = uw_1^{m_1} \cdots w_r^{m_r}$ avec u inversible, $r \geq 0$, les w_i irréductibles de l'un des types précédents et les m_i entiers positifs.

Démonstration. On en donne juste une indication, voir [1] ou [4] pour des détails. La recette est l'utilisation de la "norme" définie par $N(a + ib) = (a+bi)(a-bi) = a^2+b^2$, qui est positive et multiplicative. Ainsi, par exemple, si z est inversible dans $\mathbf{Z}[i]$, on a $zw = 1$ donc $N(z)N(w) = 1$ dans $\mathbf{N}$ et cela implique $N(z) = 1$, donc $z = \pm 1, \pm i$.

Pour montrer que l'anneau est principal on montre qu'il est euclidien relativement à la norme : pour $z, w \in \mathbf{Z}[i]$, avec $w \neq 0$, il existe $q, r \in \mathbf{Z}[i]$ avec $z = wq + r$ et $N(r) \leq N(w)$ (approcher le quotient z/w par un entier de Gauss).

La décomposition unique en irréductibles résulte du fait que principal implique factoriel (seule l'unicité pose problème, voir [1]). Enfin, la description des irréductibles est encore essentiellement une conséquence de la norme. On a en effet le lemme :

3. Une autre voie est d'utiliser le théorème de Minkowski sur les réseaux, voir [7] ou [3].

4. Deux éléments z, w d'un anneau sont dits associés si l'on a $z = wu$ avec u inversible.

5. À permutation près des w_i.

2.2 Lemme. *Un entier $p \in \mathbf{N}$ est réductible dans $\mathbf{Z}[i]$ si et seulement si c'est une norme, i.e. s'il est somme de deux carrés. Les nombres premiers p de $\mathbf{N}$ réductibles dans $\mathbf{Z}[i]$ sont $p = 2$ et les $p \equiv 1 \pmod 4$.*

Démonstration. Dire que p est réductible signifie qu'il s'écrit $p = zw$ avec $z, w \in \mathbf{Z}[i]$ non inversibles, donc de normes > 1. On a alors $N(p) = p^2 = N(z)N(w)$, ce qui impose $N(z) = N(w) = p$.

Enfin, dire qu'un nombre premier devient réductible dans $\mathbf{Z}[i]$, signifie que l'idéal (p) n'est plus premier ou encore que l'anneau quotient $\mathbf{Z}[i]/(p)$ n'est pas intègre. Or on a la description de cet anneau comme $\mathbf{Z}[i]/(p) \simeq \mathbf{F}_p[X]/(X^2+1)$ (où $\mathbf{F}_p$ désigne le corps $\mathbf{Z}/p\mathbf{Z}$). Il reste à préciser pour quels p le polynôme X^2+1 est réductible sur $\mathbf{F}_p$ c'est-à-dire pour quels p le nombre -1 est un carré de $\mathbf{F}_p$. On montre qu'il s'agit de $p = 2$ et des p congrus à 1 modulo 4, voir [1] Ch. 3.

2.3 *Remarques.* 1) Le fait que $\mathbf{Z}[i]$ soit principal sera notamment utilisé ici *via* le "lemme d'Euclide" : si un irréductible divise un produit, il divise l'un des facteurs.

2) Si p est congru à 1 modulo 4 il s'écrit $p = \alpha^2 + \beta^2$ avec $\alpha, \beta \in \mathbf{N}^*$ distincts et on peut supposer $\alpha < \beta$.

3) Les éléments $\alpha + \beta i$ et $\alpha - \beta i$ du type 2) ne sont pas associés mais $\beta + \alpha i$, par exemple, est associé à $\alpha - \beta i$ (on a $\beta + \alpha i = i(\alpha - \beta i)$). En revanche $1 + i$ et $1 - i$ sont associés car on a $1 - i = -i(1 + i)$.

Le théorème suivant fait le point sur les sommes de deux carrés :

2.4 Théorème. *Soit N un entier positif décomposé en produit de facteurs premiers :*

$$N = q_1^{m_1} \cdots q_r^{m_r} p_1^{n_1} \cdots p_s^{n_s} 2^l$$

avec les q_j (resp. les p_j) congrus à -1 (resp. 1) modulo 4. On écrit $p_j = \alpha_j^2 + \beta_j^2$ avec $\alpha_j, \beta_j \in \mathbf{N}^*$ et $\alpha_j < \beta_j$. On pose $w_j = \alpha_j + i\beta_j$.

1) Si N est somme de deux carrés, les entiers m_j sont pairs.

2) Inversement, si les m_j sont pairs, $m_j = 2m'_j$, N est somme de deux carrés d'entiers positifs ou nuls, $N = x^2 + y^2$ avec $x = |X|$, $y = |Y|$ et :

$$X + iY = \epsilon q_1^{m'_1} \cdots q_r^{m'_r} w_1^{n_{11}} \overline{w_1}^{n_{12}} \cdots w_s^{n_{s1}} \overline{w_s}^{n_{s2}} (1+i)^l$$

où ϵ est égal à 1 ou i et où les n_{jk} sont des entiers positifs ou nuls vérifiant $n_{j1} + n_{j2} = n_j$.

2.5 *Remarque.* L'énoncé précédent donne toutes les écritures possibles de N comme sommes de deux carrés, mais on y trouve à la fois les décompositions

$x^2 + y^2$ et $y^2 + x^2$ (grace à la multiplication par i) et on peut les obtenir plusieurs fois [6] (par exemple en échangeant tous les n_{j1} et n_{j2}). Une étude attentive montre qu'il y a exactement $\lceil M/2 \rceil$ décompositions distinctes $N = x^2 + y^2$ avec $x^2 \leq y^2$ où l'on a posé $M = (n_1 + 1) \cdots (n_s + 1)$ et où le symbole $\lceil x \rceil$ désigne la partie entière supérieure de x.

Démonstration. 1) Supposons $N = x^2 + y^2 = (x + iy)(x - iy)$. Soit q un facteur premier de N congru à -1 modulo 4 et m son exposant, Il s'agit de montrer que m est pair. On raisonne par récurrence sur m, le cas $m = 0$ étant évident. Le nombre q est irréductible dans $\mathbf{Z}[i]$ en vertu de 2.1, donc q divise $x + iy$ ou $x - iy$ par le lemme d'Euclide. Comme q est réel il divise x et y. On a donc $x = qx'$, $y = qy'$, $N = q^2(x'^2 + y'^2)$ et on conclut par l'hypothèse de récurrence appliquée à $N' = x'^2 + y'^2$.

2) En tenant compte de $p_j = w_j\overline{w_j}$, on vérifie que $X^2 + Y^2 = (X + iY)(X - iY)$ est égal à N, de sorte que les expressions annoncées donnent des décompositions de N en sommes de deux carrés.

Inversement, on écrit $N = X^2 + Y^2 = (X + iY)(X - iY)$ avec $X, Y \in \mathbf{Z}$ et on va montrer par récurrence sur N que X, Y sont donnés par les formules ci-dessus. Si N est égal à 1 on a les deux décompositions [7] $1 = 0^2 + 1^2 = 1^2 + 0^2$. Par ailleurs, on a $r = s = l = 0$, le produit dans l'expression de $X + iY$ est vide, donc vaut 1, et on a $X + iY = 1$, qui donne $X = 1, Y = 0$ ou $X + iY = i$ qui donne $X = 0$ et $Y = 1$, d'où le résultat.

Supposons le résultat prouvé pour tous les entiers $< N$ et passons à N. Si N admet un facteur premier $q \equiv -1 \pmod 4$, q est irréductible dans $\mathbf{Z}[i]$ donc divise $X + iY$ ou $X - iY$. Comme q est réel il divise X et Y. Si l'on pose $X = qX'$, $Y = qY'$ et $N = q^2N'$, on a $N' = X'^2 + Y'^2$ et on applique l'hypothèse de récurrence avec N'.

Si N admet un facteur premier $p \equiv 1 \pmod 4$, on écrit $p = \alpha^2 + \beta^2$ avec $0 < \alpha < \beta$ et on pose $w = \alpha + i\beta$. Cet élément est irréductible, donc divise $X + iY$ ou $X - iY$. Si w divise $X + iY$ on a $X + iY = (\alpha + i\beta)(X' + iY')$, et $N = pN'$ avec $N' = X'^2 + Y'^2$ à qui on applique l'hypothèse de récurrence. Si w divise $X - iY$, $\overline{w}$ divise $X + iY$ et on conclut de la même manière.

Enfin, si N n'a aucun facteur premier impair on a $N = 2^l = (-i)^l(1 + i)^{2l}$. Dans ce cas, $1 + i$ divise obligatoirement $X + iY$. En effet, s'il divise $X - iY$, $1 - i$ aussi car ils sont associés, donc $1 + i$ divise $X + iY$. On a donc $X + iY = (1 + i)(X' + iY')$. En écrivant $N = 2N'$ on a $X'^2 + Y'^2 = N'$ et on conclut par l'hypothèse de récurrence.

6. On notera que les complexes $\pm X \pm iY$ et $\pm Y \pm iX$ donnent tous la même décomposition $X^2 + Y^2$.

7. C'est ici que le facteur ϵ est essentiel.

2.6 *Exemple.* Si l'on considère $N = 29250 = 3^2 \times 5^3 \times 13 \times 2$, on décompose $5 = 1^2 + 2^2$ et $13 = 2^2 + 3^2$ et (en oubliant le facteur ϵ) on obtient les quatre expressions :

$$X + iY = 3(1+2i)^3(2+3i)(1+i) = 63 - 159i,$$

$$X + iY = 3(1+2i)^2(1-2i)(2+3i)(1+i) = -165 + 45i,$$

$$X + iY = 3(1+2i)^3(2-3i)(1+i) = -171 + 3i \quad \text{et}$$

$$X + iY = 3(1+2i)^2(1-2i)(2-3i)(1+i) = 105 + 135i$$

qui donnent les décompositions $29250 = 63^2+159^2 = 165^2+45^2 = 171^2+3^2 = 105^2 + 135^2$.

2.2 Rappels sur le cas $k = 1$

Ce cas est classique, c'est celui de l'équation "de Pythagore" qui admet la solution $3, 4, 5$ bien connue des charpentiers. Précisément, on a le résultat suivant :

2.7 Théorème. *Les solutions primitives dans* $\mathbf{N}$ *de l'équation* $x^2 + y^2 = z^2$ *sont exactement les triplets* $(x, y, z) \in \mathbf{N}^3$ *de l'une des deux formes suivantes :*

$$x = a^2 - b^2,\ y = 2ab,\ z = a^2 + b^2 \quad \text{ou} \quad x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2$$

où a *et* b *sont des entiers non nuls, premiers entre eux, non tous deux impairs et vérifiant* $a > b$.

On obtient toutes les solutions entières de l'équation en multipliant x, y, z *par un même entier* $d \in \mathbf{N}^*$.

Démonstration. Il y a beaucoup de démonstrations élémentaires de ce résultat, voir par exemple [2] Ch. 1, Problème 1. Nous donnons ici une preuve utilisant l'anneau $\mathbf{Z}[i]$ et le théorème 2.4. Soit $x, y, z \in \mathbf{N}$ une solution primitive (donc différente de $(0, 0, 0)$) de l'équation. Notons déjà que le cas $z = 1$ est évident, les seules solutions étant $x = 1, y = 0$ ou l'inverse. On suppose donc $z > 1$.

Si x et y sont pairs, z aussi et la solution n'est pas primitive. S'ils sont tous deux impairs, $x^2 + y^2$ est congru à 2 modulo 4 et n'est pas un carré. On en conclut que x ou y est pair et l'autre impair et que z est impair.

Si z admet un facteur premier q congru à -1 modulo 4, il est à une puissance paire dans z^2 et le théorème 2.4 montre que q divise à la fois x et y, ce qui est absurde car la solution est primitive.

Le nombre z s'écrit donc $z = p_1^{n_1} \cdots p_s^{n_s}$ où les p_j sont des nombres premiers congrus à 1 modulo 4 distincts et on a $z^2 = p_1^{2n_1} \cdots p_s^{2n_s}$.

On note ensuite que x et y sont premiers entre eux dans $\mathbf{Z}$ (sinon, un facteur premier commun diviserait aussi z contrairement à l'hypothèse). Il en résulte que $x+iy$ et $x-iy$ sont premiers entre eux dans $\mathbf{Z}[i]$ en vertu du lemme suivant :

2.8 Lemme. *Soient $x, y \in \mathbf{N}$ des entiers premiers entre eux. On suppose que x ou y est pair et l'autre impair. Alors $x+iy$ et $x-iy$ sont premiers entre eux dans $\mathbf{Z}[i]$.*

Démonstration. Sinon, soit w premier de $\mathbf{Z}[i]$ qui divise $x+iy$ et $x-iy$.

1) Si $w = q$ est un nombre premier de $\mathbf{N}$ congru à -1 modulo 4, il est réel donc divise x et y et c'est absurde.

2) Si w est de la forme $w = \alpha + i\beta$ avec $\alpha^2+\beta^2 = p$ premier de $\mathbf{N}$ congru à 1 modulo 4, comme w divise $x-iy$, $\overline{w}$ divise $x+iy$ et comme w et $\overline{w}$ sont premiers entre eux, $p = w\overline{w}$ divise $x+iy$. Comme il est réel, il divise x et y.

3) Enfin, si $w = 1+i$ on a $x+iy = (1+i)(a+ib) = a-b+i(a+b)$ et $x = a-b$ et $y = a+b$ sont de même parité.

On applique alors le théorème 2.4 en écrivant $p_j = \alpha_j^2+\beta_j^2$ comme somme de carrés avec $0 < \alpha_j < \beta_j$ et en posant $w_j = \alpha_i + i\beta_j$. Il résulte de 2.4 qu'on a $(x+iy)(x-iy) = z^2 = w_1^{2n_1}\overline{w_1}^{2n_1}\cdots w_s^{2n_s}\overline{w_s}^{2n_s}$ et comme $x+iy$ et $x-iy$ sont premiers entre eux, si un facteur w_j ou $\overline{w_j}$ divise l'un, il en est de même de $w_j^{2n_j}$ ou $\overline{w_j}^{2n_j}$. Cela signifie que $x+iy$ et $x-iy$ sont des carrés, à un inversible près. En écrivant $x+iy = \pm(a+ib)^2$ ou $x+iy = \pm i(a+ib)^2$ et en échangeant au besoin a et b ou en changeant leurs signes on a le résultat annoncé. On note que a et b sont premiers entre eux (sinon, un facteur commun divise à la fois x, y et z).

3 L'équation (E_k) : le cas où k n'est pas somme de deux carrés

3.1 Proposition. *Si $k \in \mathbf{N}^*$ n'est pas somme de deux carrés, l'équation $x^2+y^2 = kz^2$ n'a pas de solution dans $\mathbf{N}^3$ autre que $(0,0,0)$.*

Démonstration. On applique le théorème 2.4. Si k n'est pas somme de deux carrés, il admet un facteur premier congru à -1 modulo 4 à un exposant impair et cela vaut aussi pour kz^2 pour $z \neq 0$, qui n'est donc pas somme de deux carrés, donc ne s'écrit pas x^2+y^2.

3.2 *Remarque.* Dans le cas où k est congru à -1 modulo 4, par exemple $k = 31$ comme dans le problème de l'APM, il n'y a pas besoin du théorème 2.4, voir prop. 1.2. Bien entendu, ce cas particulier ne règle pas tout. Ainsi,

21, pourtant congru à 1 modulo 4, n'est pas somme de deux carrés (car on a $21 = 3 \times 7$ avec 3 et 7 congrus à -1 modulo 4). L'équation $x^2 + y^2 = 21z^2$ n'a donc pas de solution entière non nulle.

4 L'équation (E_k) : le cas où k est somme de deux carrés

4.1 Des solutions

Si $k = \alpha^2 + \beta^2$ avec $\alpha, \beta \in \mathbf{N}$ l'équation $x^2 + y^2 = kz^2$ admet une solution non nulle évidente : $x = \alpha$, $y = \beta$ et $z = 1$ et on en obtient d'autres en utilisant l'identité de Lagrange, comme on l'a vu en 1.3.1. Dans le cas présent, à partir d'une écriture de k comme somme de deux carrés et d'une une solution (u, v, z) de $u^2 + v^2 = z^2$ dans $\mathbf{N}^3$, on obtient deux solutions de (E_k) : $x = |\alpha u - \beta v|$, $y = \alpha v + \beta u$, z mais aussi, en changeant v en $-v$, $x = \alpha u + \beta v$, $y = |\alpha v - \beta u|$, z.

4.2 Toutes les solutions

La question sérieuse est de trouver toutes les solutions. Avec le premier membre $x^2 + y^2$, elle est relativement facile car l'anneau $\mathbf{Z}[i]$ est principal. Il n'en serait pas de même avec une équation de la forme $x^2 + dy^2 = z^2$, voir §5 ci-dessous. Le résultat c'est que toutes les solutions s'obtiennent par le procédé ci-dessus :

4.1 Théorème. *Soit k un entier somme de deux carrés. Les solutions de l'équation $x^2 + y^2 = kz^2$ dans $\mathbf{Z}$ sont de la forme $x = \alpha u - \beta v$, $y = \alpha v + \beta u$ où $k = \alpha^2 + \beta^2$ est une décomposition en carrés de k avec $\alpha, \beta \in \mathbf{N}$ et où (u, v, z) est une solution dans $\mathbf{Z}^3$ de l'équation $u^2 + v^2 = z^2$.*

Si u, v, z est une solution primitive de l'équation de Pythagore et si z est premier avec k, les solutions ci-dessus sont primitives.

4.2 *Remarques.* 1) Le résultat peut être formulé dans $\mathbf{Z}[i]$ sous forme de l'égalité $x + iy = (\alpha + i\beta)(u + iv)$.

2) Il suffit de montrer le résultat en oubliant la condition $\alpha, \beta \geq 0$. En effet, si l'on a une écriture sous la forme annoncée avec $\alpha, \beta \in \mathbf{Z}$ on en déduit une avec $\alpha, \beta \in \mathbf{N}$ de la façon suivante. Si α, β sont tous deux négatifs on remplace u, v par leurs opposés. Si α est positif mais $\beta < 0$ on les remplace par $|\beta|, \alpha$ et on prend $U = v$ et $V = -u$, si α est négatif et β positif on les remplace par β et $|\alpha|$ et on prend $U = -v$ et $V = u$.

Démonstration. On raisonne par récurrence sur k, le cas $k = 1$ étant évident. On écrit $(x + iy)(x - iy) = kz^2$.

1) Si k admet un facteur premier $q \equiv -1 \pmod 4$, il est à une puissance paire. Comme q est irréductible dans $\mathbf{Z}[i]$ il divise $x+iy$ ou $x-iy$ et comme il est réel il divise x et y. On a donc $x = qx'$, $y = qy'$, $k = q^2k'$ et $x'^2+y'^2 = k'z^2$ et le nombre k' est encore somme de deux carrés. On applique l'hypothèse de récurrence avec k' : il existe $\alpha', \beta' \in \mathbf{Z}$ avec $k' = \alpha'^2 + \beta^2$ et $u, v, z \in \mathbf{Z}$ vérifiant $u^2 + v^2 = z^2$ tels que $x' = \alpha' u - \beta' v$ et $y' = \alpha' v + \beta' u$. On a alors les formules annoncées avec $\alpha = q\alpha'$ et $\beta = q\beta'$.

2) Si k admet un facteur premier $p \equiv 1 \pmod 4$, on a $k = pk'$, p s'écrit $a^2 + b^2$ et k' est encore une somme de carrés. On pose $w = a + ib$. Le nombre w est irréductible dans $\mathbf{Z}[i]$ donc divise $x + iy$ ou $x - iy$.

• Si w divise $x + iy$ on écrit $x + iy = (a + ib)(x' + iy')$ et on a $x^2 + y^2 = (a^2 + b^2)(x'^2 + y'^2)$. On en déduit $x'^2 + y'^2 = k'z^2$. L'hypothèse de récurrence montre que l'on a $x' + iy' = (\alpha' + i\beta')(u + iv)$ où (u, v, z) est une solution de l'équation de Pythagore et où l'on a $k' = \alpha'^2 + \beta'^2$. Si l'on pose $\alpha + i\beta = (a + ib)(\alpha' + i\beta')$, on a $k = \alpha^2 + \beta^2$ et $x + iy = (\alpha + i\beta)(u + iv)$ comme annoncé.

• Si w divise $x-iy$, $\overline{w}$ divise $x+iy$. On écrit alors $x+iy = (a-ib)(x'+iy')$ et on conclut comme précédemment.

3) On suppose que k n'admet aucun facteur premier impair. On a donc $k = 2^l = (-i)^l(1 + i)^{2l}$. Dans ce cas, $1 + i$ divise $x + iy$ comme on l'a vu dans la preuve de 2.4. On a donc $x + iy = (1 + i)(x' + iy')$. En écrivant $k = 2k'$ on a $x'^2 + y'^2 = k'z^2$ et on conclut par l'hypothèse de récurrence.

Montrons l'assertion sur les solutions primitives. Supposons qu'un nombre premier p divise x, y, z. On a $x = \alpha u - \beta v$ et $y = \alpha v + \beta u$, donc $\alpha x + \beta y = (\alpha^2 + \beta^2)u = ku$. Le nombre p divise le premier membre. Comme k et z sont premiers entre eux, il ne divise pas k, donc il divise u. On montre de même qu'il divise v en utilisant $\alpha y - \beta x$. Mais cela contredit le fait que u, v, z est une solution primitive.

4.3 *Remarques.* 1) Pour avoir les solutions dans $\mathbf{N}$ il suffit de prendre les valeurs absolues des solutions précédentes.

2) Si k et z ont un facteur commun, les solutions données peuvent ne pas être primitives, voir remarque 1.7 ci-dessus.

3) Si x, y, z est une solution primitive de $x^2+y^2 = kz^2$, z est impair. Sinon, le second membre est multiple de 4 donc aussi le premier et cela impose x et y pairs. De plus, z n'a pas de diviseur premier congru à -1 modulo 4. Sinon, q divise $x^2 + y^2$, donc $x + iy$ ou $x - iy$, donc x et y et c'est absurde.

4.4 Corollaire. *Soit k un entier somme de deux carrés. L'équation (E_k) : $x^2 + y^2 = kz^2$ admet une infinité de solutions primitives.*

Démonstration. Cela résulte du fait que l'équation de Pythagore admet une infinité de solutions primitives.

4.3 Exemples

Pour appliquer le théorème 4.1, il suffit de connaître les solutions de l'équation de Pythagore, qui sont décrites en 2.7 et les décompositions de k en somme de deux carrés, qui ont été vues en 2.4. Voici quelques exemples.

4.3.1 Le cas $k = 29$

On retrouve les résultats vus au paragraphe 1. On notera que le fait de pouvoir échanger les rôles de α et β permet de n'avoir plus qu'une forme de solution, voir remarque 1.4.1.

4.3.2 Un autre exemple

4.5 Proposition. *Les solutions*[8] *primitives de l'équation* $x^2+y^2 = 65z^2$ *dans* $\mathbf{N}$ *sont de la forme suivante :* $x = |4(a^2-b^2)-14\epsilon ab|$, $y = |7(a^2-b^2)+8\epsilon ab|$, $z = a^2+b^2$ *ou* $x = |a^2-b^2-16\epsilon ab|$, $y = |8(a^2-b^2)+2\epsilon ab|$, $z = a^2+b^2$ *avec* $\epsilon = \pm 1$, $a, b \in \mathbf{N}^*$, *premiers entre eux, non tous deux impairs et vérifiant* $a > b$.

Si z *est premier avec* 65, *les solutions ci-dessus sont primitives.*

Démonstration. On écrit $k = 65 = 5 \times 13$, le théorème 2.4 donne, à partir de $5 = (1+2i)(1-2i)$ et $13 = (2+3i)(2-3i)$, les deux décompositions : $65 = 16+49$ et $65 = 1+64$, donc $\alpha = 4$ et $\beta = 7$ ou $\alpha = 1$ et $\beta = 8$. Le théorème 4.1 donne le résultat.

4.6 *Exemples.* 1) Avec $a = 1$ et $b = 0$ on obtient les solutions $(8, 1, 1)$ et $(4, 7, 1)$ de (E_k).

2) Avec $a = 4$ et $b = 1$ on obtient quatre solutions : $(4, 137, 17)$; $(116, 73, 17)$; $(49, 128, 17)$ et $(79, 112, 17)$.

3) Avec $a = 2$ et $b = 1$, comme $z = 5$ n'est pas premier à k, on peut avoir des solutions non primitives (on trouve $(16, 37, 5)$; $(40, 5, 5)$; $(29, 28, 5)$ et $(35, 20, 5)$).

4.7 *Remarque.* Un traitement élémentaire de cette équation est sans doute possible, mais pas tout à fait évident. Soit x, y, z une solution primitive de l'équation. On note, comme dans le cas de 29, que 65 divise $(4x+7y)(4y+7x)$ et $(4x-7y)(4y-7x)$. On regarde le nombre premier 5, il divise l'un des

8. On identifie ici les solutions (x, y, z) et(y, x, z).

facteurs, disons $4x + 7y$. On voit qu'il ne divise pas $4x - 7y$. Il divise donc $4y - 7x$ et on pose $4x + 7y = 5u$ et $-7 + 4y = 5v$ qui donne $13x = 4u - 7v$ et $13y = 7u + 4v$. Ici, il faudrait voir que 13 divise u, v, donc $4x + 7y$ et $4y - 7x$. Si ce n'est pas vrai c'est sans doute qu'il faut utiliser 8 et 1 au lieu de 7 et 4. Le lecteur perspicace se penchera sur cette intéressante question.

5 Généraliser ?

Considérons par exemple l'équation diophantienne $x^2 + dy^2 = kz^2$, voire $x^2 + dy^2 = k$, avec $d \in \mathbf{N}^*$, $d > 1$. Là, en général, les choses sont incomparablement plus compliquées car l'anneau pertinent dans ce cas est $\mathbf{Z}[i\sqrt{d}]$ (ou plus précisément l'anneau des entiers du corps $\mathbf{Q}(i\sqrt{d})$) et cet anneau n'est presque jamais principal, voir par exemple [4] ou [7]. Voici deux exemples de difficultés nouvelles. D'abord, si un nombre $n = pq$, avec p, q premiers entre eux est de la forme $x^2 + dy^2$, ses facteurs ne le sont pas nécessairement (exemple $n = 6 = 2 \times 3$ et $d = 5$). Ensuite, si l'on a une solution de $x^2 + dy^2 = kz^2$, k n'est pas nécessairement de la forme $x^2 + dy^2$ (exemple $18 = 1^2 + 17 \times 1^2 = 2 \times 3^2$).

Pour une étude de quelques exemples de telles équations, où l'on verra apparaître leur complexité, voir [5]. Pour plus de précisions sur les formes quadratiques à coefficients rationnels ou entiers, voir [6].

Références

[1] Perrin Daniel, *Cours d'algèbre*, Ellipses, 1996.

[2] Perrin Daniel, *Mathématiques d'école*, Cassini, 2011.

[3] Perrin Daniel, *Réseaux et applications.*
`https://www.imo.universite-paris-saclay.fr/~perrin/Sevres/reseaux.pdf`

[4] Perrin Daniel, *Anneaux d'entiers des corps quadratiques imaginaires*
`https://www.imo.universite-paris-saclay.fr/~perrin/TER/anneauxd%27entiers.pdf`

[5] Perrin Daniel, *Autour de quelques équations diophantiennes*
`https://www.imo.universite-paris-saclay.fr/~perrin/CAPES/arithmetique/diophantienne.pdf`

[6] Serre Jean-Pierre, *Cours d'arithmétique*, PUF, 1970.

[7] Stewart Ian & Tall David, *Algebraic number theory*, Chapmann-Hall, 1979.