Quelques équations diophantiennes

On désigne le plus souvent sous le terme générique d'*équation diophantienne* une équation polynômiale à coefficients entiers dont on cherche les solutions entières. Plus formellement, une équation diophantienne s'écrit donc sous la forme $P(x_1,x_2,\dots,x_n)=0$ avec $P\in\mathbb{Z}[X_1,\dots,X_n]$, équation aux inconnues $x_1,x_2,\dots,x_n\in\mathbb{Z}$.

Il existe de très nombreuses familles d'équations diophantiennes, issues de problématiques d'algèbre diverses et variées. La résolution de certaines repose sur des résultats d'arithmétiques élémentaires, mais d'autres peuvent nécessiter des outils mathématiques beaucoup plus sophistiqués, voire, pour ce qui concerne le Grand Théorème de Fermat, conduire à l'une des démonstrations de mathématiques les plus difficiles de tous les temps !

Citons-en quelques-unes :

1. Étant donnés trois entiers a, b et c, chercher les solutions entières de l'équation $ax+by=c$.

2. Déterminer tous les triplets pythagoriciens, c'est-à-dire les triplets (x,y,z) d'entiers tels que $x^2+y^2=z^2$.

3. Étant donné un entier $n\geq 3$, résoudre l'équation en nombres entiers $x^n+y^n=z^n$ (Fermat).

4. Étant donné un entier d qui n'est pas un carré, résoudre l'équation (dite de Pell-Fermat) $x^2-dy^2=1$.

5. Chercher tous les couples (x,y) d'entiers tels que $x^3=y^2+2$.

Il peut être intéressant de faire d'emblée quelques constats :

1. La complexité de la résolution d'une équation diophantienne n'a strictement aucun lien direct avec l'apparente complexité de l'équation elle-même.

Par exemple, l'équation en apparence compliquée $x^4+y^2=4z^6-1$ n'a trivialement pas de solutions car une somme de deux carrés n'est jamais congrue à -1 modulo 4 (il suffit pour s'en convaincre d'envisager tous les cas), alors que déterminer toutes les solutions de l'équation $x^2-3y^2=1$ demande pas mal de travail et des outils assez lourds.

2. Comme le montre l'exemple précédent, certaines équations diophantiennes peuvent ne pas avoir de solutions pour de simples questions d'incompatibilités arithmétiques primaires. Encore faut-il savoir trouver ces incompatibilités, si tant est qu'elles existent !

Le dixième problème de Hilbert

Lors du congrès international des mathématiciens qui s'est tenu à Paris en 1900, David Hilbert dressa une liste de 23 problèmes non résolus qui, selon lui, devaient servir de fil rouge pour les recherches mathématiques à venir. Parmi ceux-ci, le dixième pose la question de savoir s'il existe un algorithme général permettant de déterminer si n'importe quelle équation diophantienne possède ou non des solutions. Ce n'est qu'en 1970 que le mathématicien russe Matiyasevich prouvera qu'un tel algorithme ne peut exister.

Ce document

Il a été rédigé de manière à pouvoir être lu avec des connaissances d'arithmétique minimales. Les paragraphes **V.** et **VII.** nécessitent toutefois de connaître la notion d'anneau euclidien, et tout particulièrement de savoir que dans un tel anneau, il y a existence et unicité d'une décomposition en puissances d'irréductibles.

I. L'équation diophantienne la plus simple : $ax+by=c$. Application à un problème quotidien.

1. Le cas général

On se donne trois entiers non nuls a, b et c, et on cherche les solutions entières de l'équation $ax+by=c$.

Soit d le pgcd de a et de b. Puisque $ax+by$ est multiple de d, l'équation n'a pas de solutions quand c n'est pas multiple de d.

Si c est multiple de d, on se ramène après simplification par d à une équation de la même forme, mais dans laquelle a et b sont premiers entre eux. Nous travaillerons désormais sur une équation simplifiée de ce type.

Le théorème de Bézout affirme l'existence d'un couple d'entiers (u,v) tels que $au+bv=1$. En multipliant par c, on trouve donc que le couple (cu,cv) est une solution particulière de notre équation.

Alors :

$$\begin{aligned} ax+by=c &\Leftrightarrow ax+by=ax_0+by_0 \\ &\Leftrightarrow a(x-x_0)=b(y_0-y) \\ &\Leftrightarrow \exists k\in\mathbb{Z} \text{ tel que } x-x_0=kb \text{ et } y_0-y=ka. \end{aligned}$$

Bien entendu, la dernière équivalence résulte du théorème de Gauss puisque b divise $a(x-x_0)$ tout en étant premier avec a.

On a donc prouvé le résultat suivant :

Théorème :

Soient a, b et c, trois entiers. On suppose que a et b sont premiers entre eux. Alors les solutions entières de l'équation $ax+by=c$ sont les couples (x,y) de la forme (x_0+kb,y_0-ka) où k est un entier quelconque et (x_0,y_0) une solution particulière de l'équation (une telle solution particulière existe bien).

2. Une variante : le problème des timbres-postes

Ici, a, b et c sont trois entiers supposés *positifs* (a et b sont encore premiers entre eux), et l'on cherche s'il existe des couples (x,y) d'entiers eux-aussi positifs tels que $ax+by=c$. On supposera $a<b$.

Ce problème illustre une situation très concrète : si l'on ne dispose que de deux types de timbres, les uns à a centimes et les autres à b centimes, pour quelles valeurs de c peut-on affranchir une lettre à c centimes ?

Nous dirons d'un entier c qu'il est *affranchissable* s'il existe deux entiers positifs x et y tels que $ax+by=c$.

Une première remarque triviale : si c est affranchissable, $c+a$ est affranchissable (il suffit de rajouter un timbre à a centimes). En conséquence, si a entiers consécutifs sont affranchissables, disons $p,p+1,\ldots,p+a-1$, alors les a entiers suivants le sont, puis par récurrence tous les entiers suivants le sont.

Soit un entier c quelconque. Comme on l'a vu plus haut, on a toutes les solutions de l'équation $ax+by=c$ sous la forme :

$$x=u-kb\ ,\ y=v+ka,\ k\in\mathbb{Z}\ ,$$

où (u,v) désigne une solution particulière de l'équation.

L'entier c est affranchissable si l'on peut remplir les conditions $x\geq 0$ et $y\geq 0$, lesquelles s'écrivent $k\leq\dfrac{u}{b}$ et $k\geq -\dfrac{v}{a}$. Mais une façon simple d'assurer l'existence d'un entier satisfaisant à ces deux conditions est de demander au segment $[-\dfrac{v}{a},\dfrac{u}{b}]$ d'être de longueur au moins égale à 1, c'est à dire d'avoir $\dfrac{u}{b}+\dfrac{v}{a}\geq 1$, soit en multipliant par ab d'avoir $au+bv=c\geq ab$: *tout entier supérieur ou égal à ab est affranchissable.*

Envisageons alors les entiers $ab+1, ab+2, \ldots, ab+a-1$: tous sont affranchissables, et comme aucun de ces nombres n'est multiple ni de a ni de b, tous doivent être affranchis avec au moins un timbre a et un timbre b.

Par ailleurs, l'entier suivant $ab+a$ peut être affranchi avec un timbre a et a timbres b. En retirant un timbre a et un timbre b à tous ces affranchissements, on en déduit que les entiers $ab+1-a-b\,, ab+2-a-b\,, \ldots, ab-b$ sont affranchissables : on en a trouvé a consécutifs, notre première remarque s'applique :

Tout entier supérieur ou égal à $ab+1-a-b$ est affranchissable.

Reste à voir, pour conclure, que $c=(a-1)(b-1)-1=ab-a-b$ n'est pas affranchissable.

On a une solution particulière de l'équation $ua+bv=c$ en prenant $u=b-1$ et $v=-1$. On a donc toutes les solutions de l'équation $ax+by=c$ sous la forme $x=b-1-kb$ et $y=-1+ka$. Les conditions $x\geq 0$ et $y\geq 0$ s'écrivent donc :

$$k\leq 1-\frac{1}{b}<1 \text{ et } k\geq \frac{1}{a}>0\,,$$

conditions qui ne sont évidemment pas compatibles si k est entier.

On a finalement résolu notre problème :

Théorème :

Soient a, b et c, trois entiers positifs. On suppose que a et b sont premiers entre eux. Alors l'entier $c=ab-a-b$ est le plus grand pour lequel l'équation $ax+by=c$ ne possède pas de solutions avec x et y entiers positifs.

II. Recherche des triplets pythagoriciens

1. Forme générale des solutions

On recherche ici tous les triplets d'entiers tels que $x^2+y^2=z^2$.

Remarquons que l'on peut générer assez facilement des solutions à cette équation. En effet, il est connu que la somme des n premiers nombres impairs est un carré, plus précisément que $1+3+\ldots+(2n-1)=n^2$. Alors, à chaque fois que l'on ajoutera à cette somme un terme de la forme $2n+1$ qui sera lui-même un carré parfait, on obtiendra une somme de deux carrés égale à un carré : par exemple,

$$5^2=1+3+5+7+9=(1+3+5+7)+9=4^2+3^2\,.$$

Par le même procédé, on peut découvrir la solution $12^2+5^2=13^2$.

Soient x, y et z trois entiers non nuls solutions de l'équation $x^2+y^2=z^2$. Si p est un nombre premier divisant deux d'entre eux, il divise le troisième. Donc, si l'on pose $d=\text{pgcd}\,(x,y)$, alors d est aussi un diviseur de z et $X=x/d\,, Y=y/d\,, Z=z/d$ sont trois entiers *deux à deux premiers entre eux* tels que $X^2+Y^2=Z^2$.

Notons que X et Y ne peuvent être simultanément impairs car, sinon, Z^2 serait un carré de la forme $4n+2$ ce qui est impossible. On supposera donc, pour fixer les idées, que X est impair et Y pair ; cela entraîne évidemment que Z est impair.

Écrivons que $\dfrac{Y^2}{4}=\dfrac{Z-X}{2}\times\dfrac{Z+X}{2}$, et constatons que $\dfrac{Z-X}{2}$ et $\dfrac{Z+X}{2}$ sont entiers et premiers entre eux puisque X et Z le sont. Leur produit étant un carré, chacun d'eux est un carré et on peut donc écrire :
$\dfrac{Z+X}{2}=u^2\,,\ \dfrac{Z-X}{2}=v^2$ avec u et v premiers entre eux.

On aboutit ainsi à :

$$Z=u^2+v^2\,,\ X=u^2-v^2\,,\ Y=2uv \ \text{(quitte à changer } u \text{ en } -u\,),$$

avec u et v premiers entre eux et de parités opposées (sinon X serait pair).

Réciproquement, on vérifie trivialement qu'un tel triplet est bien solution de l'équation de départ et que ses éléments sont deux à deux premiers entre eux avec X impair et Y pair.

Théorème :

Les solutions de l'équation $x^2+y^2=z^2$ *sont, à l'échange de* x *et de* y *près, les triplets de la forme :*

$$x=d(u^2-v^2)\,,\ y=2duv\,,\ z=d(u^2+v^2)$$

où d *est un entier quelconque, et* u *et* v *deux entiers premiers entre eux de parités opposées.*

2. Le théorème de Fermat pour $n=4$

On se propose ici de prouver que l'équation $x^4+y^4=z^2$ ne possède pas de solutions en nombres entiers non nuls. Bien évidemment, cela entraine *a fortiori* que l'équation $x^4+y^4=z^4$ n'en possède pas non plus. La démonstration qui suit utilise le procédé de *descente infinie* initié par Fermat lui-même, et qui consiste à envisager une solution de l'équation avec z minimal et d'en construire une nouvelle avec un $z'<z$, ce qui constitue bien évidemment une contradiction.

Soit donc une solution de l'équation $x^4+y^4=z^2$ avec z minimal. Cela entraine bien sûr que x et y sont premiers entre eux car si p était un diviseur premier commun à x et à y, alors p^2 diviserait z et l'on disposerait d'une solution $(\frac{x}{p},\frac{y}{p},\frac{z}{p^2})$ avec $\frac{z}{p^2}<z$.

Comme on a $(x^2)^2+(y^2)^2=z^2$, l'étude des triplets pythagoriciens précédemment effectuée permet d'affirmer que x et y sont de parités opposées, et l'on supposera par exemple x impair. On peut donc écrire :

$$x^2=u^2-v^2\,,\ y^2=2uv\,,\ z=u^2+v^2\,,$$

avec u et v premiers entre eux et de parités opposées.

Puisque u et v sont premiers entre eux et que l'on a $u^2=x^2+v^2$ avec x impair, on sait aussi que u est impair, que v est pair et que l'on peut écrire :

$$x=a^2-b^2\,,\ v=2ab \text{ et } u=a^2+b^2 \text{ avec } a \text{ et } b \text{ premiers entre eux.}$$

Puisque a et b sont premiers entre eux et que $u=a^2+b^2$, il est clair que u, a et b sont deux à deux premiers entre eux. Mais $y^2=4uab$, il en résulte donc que chacun des nombres u, a et b est un carré.

On écrit donc $u=p^2\,,\ a=q^2\,,\ b=r^2$ et il vient $q^4+r^4=p^2$.

On a donc trouvé une nouvelle solution (q,r,p) de l'équation initiale. Mais il est facile de voir que $p<z$, d'où l'impossibilité cherchée.

Théorème :

Une somme de deux puissances quatrièmes d'entiers non nuls n'est jamais un carré parfait.

III. L'équation $x^2-2y^2=1$

Il s'agit d'un cas particulier d'équation de Pell-Fermat. Ces équations de la forme $x^2-dy^2=1$ se résolvent de manière générale en utilisant la théorie des fractions continues, mais on sort alors du cadre de ce modeste document.

Comme il est évident que x ou y peut être changé en son opposé, nous chercherons ici les solutions *positives* de cette équation, c'est-à-dire les couples (x,y) d'entiers positifs vérifiant $x^2-2y^2=1$.

Remarquons que l'on dispose des solutions triviales $(1,0)$ et $(3,2)$. Avec un peu plus de persévérance, on peut découvrir la solution $(17,12)$. En réalité, il est facile à partir d'une solution d'en engendrer d'autres. En effet, on vérifie aisément que si (x,y) est une solution, $u(x,y)=(3x+4y,2x+3y)$ en est une autre[1] :

$$(3x+4y)^2-2(2x+3y)^2=9x^2+24xy+16y^2-8x^2-24xy-18y^2=x^2-2y^2=1\,.$$

Forts de ce constat, en partant de la solution triviale $(1,0)$, on trouve les solutions $(3,2)$, puis $(17,12)$, puis $(99,70)$ et ainsi de suite…

Mais, exactement de la même façon, il est facile de voir que si (x,y) est une solution, il en va de même de $v(x,y)=(3x-4y,-2x+3y)$ (en fait, il s'agit de l'opération inverse de la précédente, qui permet de "remonter" de la solution $(17,12)$ à $(3,2)$, puis à $(1,0)$, puis à… $(3,-2)$ qui est en réalité la même solution que $(3,2)$.

Lemme :

Soit (x,y) une solution positive de l'équation $x^2-2y^2=1$, autre que la solution $(1,0)$. Alors $v(x,y)=(3x-4y,-2x+3y)$ est encore une solution positive, qui vérifie en outre $3x-4y<x$.

Preuve : Comme y est non nul et ne peut valoir 1 (sinon on aurait $x^2=3$), y vaut au moins 2. Par suite :

$$y^2\geq 4=4x^2-8y^2\Rightarrow 9y^2\geq 4x^2\Rightarrow 3y\geq 2x\Leftrightarrow -2x+3y\geq 0\,.$$

De même :

$$x^2-2y^2=1\Rightarrow x^2>2y^2\Rightarrow 9x^2>18y^2>16y^2\Rightarrow 3x>4y\Leftrightarrow 3x-4y>0\,.$$

Enfin :

$$x^2=2y^2+1<4y^2\Rightarrow x<2y\Rightarrow 3x-4y<x\,.$$

De ce lemme, il ressort que quand on connaît une solution positive (x_0,y_0) autre que $(1,0)$, on sait construire une autre solution positive $(x_1,y_1)=v(x_0,y_0)$ telle que $x_1<x_0$. Posons $(x_n,y_n)=v^n(x_0,y_o)$. Si l'on a $(x_n,y_n)\neq(1,0)$ pour tout n, alors la suite (x_n) est une suite strictement décroissante d'entiers positifs, c'est impossible. Il existe donc un entier p tel que $(x_p,y_p)=v^p(x_0,y_0)=(1,0)$, ou encore tel que $(x_0,y_0)=u^p(1,0)$. Le procédé d'itération décrit au début fournit donc *toutes* les solutions positives de notre équation.

Théorème :

Les solutions entières positives de l'équation $x^2-2y^2=1$ sont les couples (x,y) obtenus à partir du couple $(1,0)$ par l'itération de la transformation $(x,y)\mapsto(3x+4y,2x+3y)$.

IV. L'équation $x^3=y^2-7$

On démontre ici de manière très élémentaire que cette équation diophantienne ne possède pas de solutions. Soit donc une solution supposée (x,y).

Remarquons que x est impair. En effet, s'il était pair, $y^2=x^3+7$ serait un carré de la forme $4n+3$, ce qui n'est pas possible.

Réécrivons l'équation sous la forme $x^3+8=y^2+1$, ou encore $(x+2)(x^2-2x+4)=y^2+1$, ou enfin $(x+2)\big((x-1)^2+3\big)=y^2+1$. L'entier $(x-1)^2+3$ étant de la forme $4n+3$ (x est impair), l'un au moins de ses

[1] Il va sans dire que la découverte de $u(x,y)$ n'a rien de miraculeux. En effet, si l'on travaille dans l'anneau $\mathbb{Z}[\sqrt{2}]$ et si $x+\sqrt{2}y$ en est une unité, le produit $(x+\sqrt{2}y)(3+2\sqrt{2})=(3x+4y)+\sqrt{2}(2x+3y)$ est encore une unité.

diviseurs premiers p est lui-même de la forme $4n+3$. Par suite, on a $y^2=-1$ dans $\mathbb{Z}/p\mathbb{Z}$ ce qui est impossible quand p est congru à 3 modulo 4. En effet, en élevant à la puissance impaire $\frac{p-1}{2}$, on obtient $y^{p-1}=(-1)^{\frac{p-1}{2}}=-1$. Mais $y^{p-1}=1$ d'après le petit théorème de Fermat, d'où l'impossibilité.

Théorème :
L'équation $x^3=y^2-7$ ne possède pas de solutions entières.

V. L'équation de Fermat $x^3=y^2+2$

Il s'agit ici de prouver que $x=3$ et $y=2$ sont les seules solutions entières positives de l'équation $x^3-2=y^2$.

L'idée pour ce faire est d'écrire cette équation $x^3=(y+\sqrt{-2})(y-\sqrt{-2})$ et de travailler dans l'anneau $\mathbb{Z}[\sqrt{-2}]$.

Soit donc (x,y) un couple de solutions de cette équation.

Lemme 1 :
L'anneau $\mathbb{Z}[\sqrt{-2}]$ est euclidien (pour le stathme $N(a+b\sqrt{-2})=\left|a+b\sqrt{-2}\right|^2=a^2+2b^2$). Le groupe de ses unités se réduit à $\{-1,1\}$.

Preuve : Soient u et v deux éléments de $\mathbb{Z}[\sqrt{-2}]$ avec v non nul. Le complexe u/v peut être localisé dans le plan complexe dans un rectangle du réseau $\mathbb{Z}[\sqrt{-2}]$, rectangle dont la demie-diagonale est de longueur $\sqrt{3}/2<1$. L'un des 4 sommets du rectangle est donc à une distance strictement plus petite que 1 de u/v, et si l'on note q ce sommet et $r=u-qv$, il vient $u=qv+r$ avec $|r|^2<|v|^2$. De plus, une unité devant être de stathme 1, on voit facilement qu'il n'y a que 1 et -1.

Lemme 2 :
Les nombres $y+\sqrt{-2}$ et $y-\sqrt{-2}$ sont premiers entre eux dans $\mathbb{Z}[\sqrt{-2}]$.

Preuve : Soit d un éventuel diviseur irréductible commun à $y+\sqrt{-2}$ et $y-\sqrt{-2}$.

Par différence, d divise $-2\sqrt{-2}=\left(\sqrt{-2}\right)^3$. Or, il est à peu près évident que $\sqrt{-2}$ est irréductible dans $\mathbb{Z}[\sqrt{-2}]$ (si $\sqrt{-2}=ab$, alors $2=N(a)\times N(b)$ et comme tout ce petit monde est entier, il vient que $N(a)$ ou $N(b)$ vaut 1). Il en résulte que d ne peut valoir que $\sqrt{-2}$ (ou $-\sqrt{-2}$, ce qui revient au même). Mais alors $\sqrt{-2}$ divise y, y est donc un entier pair, et l'équation $x^3=y^2+2$ conduit à une impossibilité en raisonnant modulo 4.

Ainsi, puisque $y+\sqrt{-2}$ et $y-\sqrt{-2}$ sont premiers entre eux dans l'anneau euclidien $\mathbb{Z}[\sqrt{-2}]$, l'égalité $x^3=(y+\sqrt{-2})(y-\sqrt{-2})$ prouve (par unicité de la décomposition en irréductibles) que ce sont chacun des cubes (à une unité multiplicative près ce qui ne change rien puisque 1 et -1 sont eux-mêmes des cubes).

Écrivons $y+\sqrt{-2}=(a+b\sqrt{-2})^3$, il vient en identifiant partie réelle et partie imaginaire que :

$$y=a^3-6ab^2 \text{ et } 1=3a^2b-2b^3=b(3a^2-2b^2).$$

La deuxième égalité prouve que $b=\pm 1$.

L'éventualité $b=-1$ conduit à $3a^2=1$ ce qui est impossible.

L'éventualité $b=1$ conduit à $a^2=1$ puis à $y=\pm 5$: on retrouve ainsi la solution évidente de notre équation, qui apparaît donc comme étant unique.

Théorème :
La seule solution en nombres entiers positifs de l'équation $x^3=y^2+2$ *est* $x=3$ *et* $y=5$.

VI. L'équation $x^2+y^2+z^2+t^2=n$

1. Le théorème de Lagrange

On démontre dans cette section que l'équation $x^2+y^2+z^2+t^2=n$ possède des solutions pour tout entier positif n, en d'autres termes que tout entier positif est somme de 4 carrés.

Lemme 1 :
Quels que soient les entiers a, b, c, d, A, B, C, D, on a :

$$(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2)$$
$$=(aA+bB+cC+dD)^2+(aB-bA-cD+dC)^2+(aC-cA+bD-dB)^2+(aD-dA-bC+cB)^2$$

Preuve : On peut bien évidemment se contenter d'une vérification ! Mais cette formule magique n'est que la transcription de l'identité classique sur les quaternions : $\left|zz'\right|^2=\left|z\right|^2\left|z'\right|^2$.

De ce lemme 1 résulte immédiatement que le produit de deux entiers sommes de 4 carrés est lui-même somme de 4 carrés. Ainsi, si l'on prouve que tout nombre premier est somme de 4 carrés, cette propriété rejaillira sur tous les entiers.

On considère donc un nombre premier p et on exclut le cas trivial $p=2$.

Lemme 2 :
Il existe un entier $m<p$ *tel que* mp *soit somme de 4 carrés.*

Preuve : dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $x^2=y^2$ s'écrit $(x-y)(x+y)=0$ et n'a donc que les solutions $x=y$ et $x=-y$ puisque l'on est dans un corps. Il en résulte que, à part 0, tout carré de $\mathbb{Z}/p\mathbb{Z}$ est le carré d'exactement deux éléments qui sont opposés l'un de l'autre. On a donc en tout $\frac{p-1}{2}+1$ carrés dans $\mathbb{Z}/p\mathbb{Z}$. De la même façon, on a $\frac{p-1}{2}+1$ éléments de $\mathbb{Z}/p\mathbb{Z}$ de la forme $1-y^2$. Comme $\frac{p-1}{2}+1+\frac{p-1}{2}+1=p+1>p$, il y a un élément commun à ces deux collections, et il existe donc x et y dans $\mathbb{Z}/p\mathbb{Z}$ tels que $x^2=1-y^2$. En remontant dans $\mathbb{Z}$ et en choisissant des entiers X et Y de résidus x et y modulo p, X et Y tous deux plus petits en valeur absolue que $\frac{p}{2}$, on peut écrire $X^2+Y^2+1=mp$ avec $m=\frac{1}{p}(X^2+Y^2+1)\leq\frac{1}{p}(\frac{p^2}{2}+1)<p$.

Considérons à partir de maintenant le plus petit entier m tel que mp soit somme de 4 carrés, et supposons que $m>1$. On écrira $mp=a^2+b^2+c^2+d^2$. En réduisant cette égalité modulo m et en remontant encore une fois dans $\mathbb{Z}$ par des choix d'entiers inférieurs à $\frac{m}{2}$ en valeurs absolues, on trouve donc 4 entiers A, B, C et D tels que $A^2+B^2+C^2+D^2$ soit multiple de m. On écrira $A^2+B^2+C^2+D^2=km$.

Si $k=0$, alors $A=B=C=D=0$, c'est-à-dire que a, b, c et d étaient multiple de m. Mais en réinjectant dans l'équation $mp=a^2+b^2+c^2+d^2$, on en déduit que p divise m ce qui est impossible puisque $m<p$.

Par ailleurs, $k=\dfrac{1}{m}(A^2+B^2+C^2+D^2)\leq\dfrac{1}{m}4\dfrac{m^2}{4}=m$. Mais k ne peut valoir m que si chacun des nombres A, B, C et D vaut en valeur absolue $\dfrac{m}{2}$. Alors a^2, b^2, c^2 et d^2 sont tous congrus à $\dfrac{m^2}{4}$ modulo m et on retrouve comme précédemment que p divise m, c'est impossible.

Tous ces efforts pour arriver à la conclusion que $0<k<m$ *!*

Multiplions maintenant entre elles les égalités $mp=a^2+b^2+c^2+d^2$ et $A^2+B^2+C^2+D^2=km$ en utilisant la formule du lemme 1. On obtient :

$$kpm^2=\alpha^2+\beta^2+\gamma^2+\delta^2\,,$$

avec :

$$\begin{cases}\alpha=aA+bB+cC+dD\equiv a^2+b^2+c^2+d^2=mp\equiv 0\ [m]\\ \beta=aB-bA+cD-dC\equiv ab-ab+cd-cd\equiv 0\ [m]\\ \gamma \text{ et } \delta \text{ congrus à 0 modulo } m \text{ pour les mêmes raisons que } \beta\end{cases}$$

Finalement, après simplification par m^2, on trouve donc que kp est une somme de 4 carrés avec $k<m$, ce qui contredit le caractère minimal de m.

Théorème (Lagrange) :
Tout entier positif est somme de 4 carrés.

2. Sommes de puissance quatrièmes

On vérifie aisément qu'en posant $\sigma(x,y)=(x+y)^4+(x-y)^4$, alors on a l'identité :

$$6(a^2+b^2+c^2+d^2)^2=\sigma(a,b)+\sigma(a,c)+\sigma(a,d)+\sigma(b,c)+\sigma(b,d)+\sigma(c,d)\,.$$

Soit alors un entier N supposé être multiple de 6, $N=6n$. En décomposant n en somme de 4 carrés, on écrit dans un premier temps $N=6(p^2+q^2+r^2+s^2)$. Puis, chacun à son tour, les entiers p, q, r et s peuvent être décomposés en somme de 4 carrés. Grâce à l'identité précédente, on décompose donc N en somme de 48 puissances quatrièmes.

Dans le cas général où N n'est pas supposé être multiple de 6, on écrit $N=6k+r$ avec $r=0,1,2,3,4$ ou 5, et l'on voit ainsi que N est somme de 53 puissances quatrièmes.

Théorème (Liouville) :
Tout entier positif est somme de 53 puissances quatrièmes.

VII. L'équation $z=x^2+y^2$

On prouve dans ce paragraphe que, z étant un entier, l'équation $z=x^2+y^2$ possède des solutions si et seulement si les nombres premiers de la forme $4n+3$ figurant dans la décomposition en facteurs premiers de z sont tous élevés à une puissance paire.

Lemme 1 :

L'anneau $\mathbb{Z}[\mathrm{i}]$ *des entiers de Gauss est euclidien (pour le stathme* $N(a+\mathrm{i}b)=\left|a+\mathrm{i}b\right|^2=a^2+b^2$*). Ses unités sont* 1, -1, i *et* $-\mathrm{i}$.

Preuve : Soient u et v deux éléments de $\mathbb{Z}[\mathrm{i}]$ avec v non nul. Le complexe u/v peut être localisé dans le plan complexe dans un carré du réseau $\mathbb{Z}[\mathrm{i}]$, rectangle dont la demie-diagonale est de longueur $\sqrt{2}/2 < 1$. L'un des 4 sommets du carré est donc à une distance strictement plus petite que 1 de u/v, et si l'on note q ce sommet et $r = u - qv$, il vient $u = qv + r$ avec $|r|^2 < |v|^2$. De plus, une unité devant être de stathme 1, on voit facilement qu'il n'y a que 1, -1, i et $-\mathrm{i}$.

Lemme 2 :

Pour p premier de la forme $4n+1$, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Preuve : Il existe plusieurs preuves classiques de ce résultat. Nous allons en choisir une moins répandue, qui a le mérite en outre d'être constructive.

Soit donc p un nombre premier de la forme $4n+1$. D'après le théorème de Wilson, $(p-1)! \equiv -1\ [p]$. Regroupons dans la factorielle chaque terme avec son opposé : 1 avec $p-1$, 2 avec $p-2$ etc. On obtient ainsi un produit de $\dfrac{p-1}{2}$ termes qui sont tous des opposés de carrés, on peut donc écrire $(p-1)! \equiv (-1)^{\frac{p-1}{2}} a^2 \equiv -1\ [p]$, et donc $a^2 \equiv -1\ [p]$.

Remarque : On a prouvé, dans le paragraphe **IV**, que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$ quand p est premier de la forme $4n+3$.

Lemme 3 :

Un nombre premier p est somme de deux carrés si et seulement $p = 2$ ou p est de la forme $4n+1$.

Preuve : Une somme de deux carrés étant toujours congrue à 0, 1 ou 2 modulo 4, un nombre premier de la forme $4n+3$ ne saurait être somme de deux carrés (comme d'ailleurs tout entier de cette forme, qu'il soit premier ou non). Par ailleurs, 2 est évidemment somme de deux carrés.

Soit maintenant un nombre premier p de la forme $4n+1$. D'après le lemme 2, -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, il existe donc deux entiers x et k tels que $x^2 + 1 = kp$, soit $kp = (x+\mathrm{i})(x-\mathrm{i})$. Si p était irréductible dans $\mathbb{Z}[\mathrm{i}]$ qui est euclidien, il diviserait l'un des deux termes $x+\mathrm{i}$ ou $x-\mathrm{i}$, donc l'autre puisque ceux-ci sont conjugués. Finalement, il diviserait leur somme qui vaut $2\mathrm{i}$, et on aurait donc $p = 2$ ce qui est exclu. Ainsi, p n'est pas irréductible dans $\mathbb{Z}[\mathrm{i}]$ et l'on peut écrire $p = ab$ avec a et b deux entiers de Gauss qui ne sont pas des unités, donc de normes différentes de 1. Prenons les modules au carré : $p^2 = N(a)N(b)$, et donc $N(a) = N(b) = p$. Reste à écrire $a = \alpha + \mathrm{i}\beta$ et il vient $p = \alpha^2 + \beta^2$: p est somme de deux carrés.

Lemme 4 :

Les irréductibles de $\mathbb{Z}[\mathrm{i}]$ sont les entiers de Gauss de la forme $x+\mathrm{i}y$ avec $x+\mathrm{i}y$ premier, ainsi que les nombres premiers de la forme $4n+3$.

Preuve : Soit $x+\mathrm{i}y$ un entier de Gauss avec x^2+y^2 premier. Si $x+\mathrm{i}y = zz'$, il vient en prenant les modules au carré $x^2+y^2 = |z|^2 |z'|^2$. Comme x^2+y^2 est premier, cela entraine par exemple que $|z|^2 = 1$; z est donc une unité et $x+\mathrm{i}y$ est bien irréductible.

Soit maintenant un nombre premier q de la forme $4n+3$. Si $q = zz'$, on a $q^2 = |z|^2 |z'|^2$. Mais on ne peut avoir $q = |z|^2$ car sinon, q serait somme de deux carrés ce qui est impossible quand q est de la forme $4n+3$. On a donc par exemple $|z|^2 = 1$ et q est irréductible.

Lemme 5 :

Quels que soient les entiers a, b, c, d, on a $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$.

Preuve : la vérification est immédiate. Cette formule résulte bien évidemment du fait que si z et z' sont deux complexes, on a $\left|zz'\right|^2=\left|z\right|^2\left|z'\right|^2$.

Le lemme 5 prouve que le produit de deux nombres qui sont sommes de deux carrés est un nombre qui est somme de deux carrés. 2 et les nombres premiers de la forme $4n+1$ étant des sommes de deux carrés, on en déduit aisément qu'un entier dont les facteurs premiers de la forme $4n+3$ sont tous élevés à une puissance paire est une somme de deux carrés.

Inversement, soit N un entier somme de deux carrés, $N=a^2+b^2=(a+\mathrm{i}b)(a-\mathrm{i}b)$. Décomposons $a+\mathrm{i}b$ en produit d'irréductibles dans $\mathbb{Z}[\mathrm{i}]$. On obtient alors par conjugaison la décomposition de $a-\mathrm{i}b$. Quoi qu'il en soit, chaque facteur irréductible de la forme q premier avec q congru à 3 modulo 4 apparaîtra à la fois dans $a+\mathrm{i}b$ et dans $a-\mathrm{i}b$, et il apparaîtra donc avec une puissance paire dans N.

On a donc enfin prouvé le résultat annoncé en début de paragraphe :

Théorème (dit des deux carrés) :

Un entier z est somme de deux carrés si et seulement si les nombres premiers de la forme $4n+3$ *figurant dans la décomposition en facteurs premiers de z sont tous élevés à une puissance paire.*