Résolution élémentaire de quelques équations diophantiennes

par Richard Antetomaso

comité de rédaction de la RMS

RÉSUMÉ. *On étudie les équations diophantiennes ($x^4 - 3y^4 = 1, x^4 - 12y^4 = 1, x^2 - 12y^4 = 1$) par la méthode de descente infinie de Fermat et on en déduit une résolution élémentaire de l'équation $y^3 = x^2 + 1$.*

ABSTRACT. Resolution of some diophantine equations by elementary means

We study the diophantine equations ($x^4 - 3y^4 = 1, x^4 - 12y^4 = 1, x^2 - 12y^4 = 1$) by Fermat's method of descent, from which we give an elementary resolution of the equation $y^3 = x^2 + 1$.

MOTS-CLÉS : *équations diophantiennes, descente infinie de Fermat, équations de Mordell.*

1. Introduction

1.1. *Objectif*

Plusieurs lecteurs ayant résolu l'exercice 3 publié dans ce numéro se sont demandé si une preuve élémentaire (i.e. n'utilisant que l'arithmétique de $\mathbb{Z}$) du théorème suivant était possible :

Théorème 1. — *Le couple $(0, 1)$ est la seule solution dans $\mathbb{Z}^2$ de $y^3 = x^2 + 1$.*

On reconnaît là une équation de Mordell-Bachet, voire un cas très particulier de la conjecture de Catalan, qui est résolue classiquement à l'aide de l'arithmétique de l'anneau $\mathbb{Z}[i]$ dans ce numéro (voir la correction de l'exercice 3 de ce numéro). Dans cette note nous proposons une preuve élémentaire du **théorème 1** nous appuyant sur la résolution des équations diophantiennes

$$(E_3) : x^4 - 3y^4 = 1, \quad (F_3) : x^4 - 12y^4 = 1 \text{ et } (G_{12}) : x^2 - 12y^4 = 1$$

Précisément nous établirons le

Théorème 2. — *Les équations* (E_3), (F_3) *et* (G_{12}) *admettent* $(1,0)$ *comme seule solution dans* $\mathbb{N}^2$.

1.2. *Remarques*

• La preuve qui suit est élémentaire dans la mesure où elle utilise seulement la factorisation dans $\mathbb{N}^*$ et quelques congruences.

• La preuve du **théorème 1** repose sur une descente infinie : on part d'une solution et on en déduit une strictement plus petite, ce qui dans $\mathbb{N}$ ne peut pas être indéfiniment itéré. Elle est néanmoins rédigée en termes de récurrence, conformément aux habitudes pédagogiques actuelles.

On notera aussi que la descente se fait sur les deux équations E_3 et F_3 à la fois : une solution de l'une conduit à une solution plus petite de l'autre.

2. Un lemme simple

Lemme 1. — *Si* x *est un entier impair alors* $x^2 \equiv 1$ *mod* 8 *et* $x^4 \equiv 1$ *mod* 16.

En effet, si $x = 2k+1$, on a alors $x^2 = 4k(k+1)+1 \equiv 1 \bmod 8$. Puis, en posant $x^2 = 8p+1$, $x^4 = (8p+1)^2 = 64p^2 + 16p + 1 \equiv 1 \bmod 16$.

3. Preuve du théorème 2

3.1. *Cas de* E_3 *et* F_3

Nous allons faire une preuve par « descente infinie » sur les deux équations E_3 et F_3 à la fois. Précisément on prouve par récurrence sur N que si (x,y) est solution de l'une des deux équations avec $x \leqslant N$, alors $x = 1$.

C'est vrai pour $N = 1$. Supposons l'énoncé vrai pour $N = x - 1 \geqslant 1$ et supposons (x,y) solution de l'une des équations.

• Si $x^4 - 3y^4 = 1$, alors x est impair car sinon $x^4 \equiv 0 \bmod 16$ et $-3y^4 \equiv 1 \bmod 16$, ce qui n'est pas possible. Par suite y est pair.

De plus on a $(x^2-1)(x^2+1) = 3y^4$ avec x^2+1 multiple de 2 mais ni de 4 ni de 3 (car -1 n'est pas un carré modulo 3 ou 4). Le pgcd de x^2-1 et $x^2+1 = x^2-1+2$ est donc 2. En outre 2^4 divise y^4 donc x^2-1 est multiple de 8. Ainsi $\dfrac{x^2-1}{24}$ et $\dfrac{x^2+1}{2}$ sont premiers entre eux et leur produit est $\left(\dfrac{y}{2}\right)^4$, donc il existe a, b premiers entre eux tels que

$$x^2 - 1 = 24a^4, \quad x^2 + 1 = 2b^4.$$

On en déduit $b^4-12a^4=1$. Remarquons que $x\neq 0$. On vérifie alors aisément que $\dfrac{x^2+1}{2}<x^4$ pour tout $x\in\mathbb{N}^\star$, c'est-à-dire $b<x$ et l'hypothèse de récurrence assure $b=1$. On a donc aussi $x=1$.

• Si $x^4-12y^4=1$ alors x est impair. Par suite x^2-1 est multiple de 8 donc y est pair.

De plus on a $(x^2-1)(x^2+1)=12y^4$ avec x^2+1, comme précédemment, multiple de 2 mais ni de 4 ni de 3 et le pgcd de x^2-1 et x^2+1 égal à 2. On déduit par un raisonnement analogue qu'il existe a,b premiers entre eux tels que

$$x^2+1=2b^4 \text{ et } x^2-1=3.2^5a^4=6c^4 \text{ où } c=2a,$$

d'où $b^4-3c^4=1$. Comme $b<x$, l'hypothèse de récurrence assure $b=1$. On a donc aussi $x=1$.

3.2. *Cas de* G_{12}

Si $x^2-12y^4=1$ alors on a deux cas possibles :

• $x-1=6a^4, x+1=2b^4$ d'où $1=b^4-3a^4$ puis $b=1, a=0$ (car $(1,0)$ est la seule solution de (E_3)) et donc $x=1, y=0$.

• $x-1=2a^4, x+1=6b^4$ d'où $1=3b^4-a^4$. Comme les puissances quatrièmes modulo 16 sont 0 et 1, la congruence $3b^4\equiv a^4+1 \bmod 16$ est impossible.

4. Preuve du théorème 1

4.1. *La seule solution dans* $\mathbb{N}^2$ *de l'équation* $x^4-6x^2y^2-3y^4=1$ *est* $(x,y)=(1,0)$.

On peut l'écrire $(x^2-3y^2)^2-12y^4=1$. Comme $(1,0)$ est la seule solution dans $\mathbb{N}^2$ de G_{12} on a $x=1$ et $y=0$.

4.2. *Fin de la preuve*

Supposons que $(x,y)\in\mathbb{N}^2$ vérifie $x^2+1=y^3$. On peut écrire $x^2=(y-1)(y^2+y+1)$.

Comme $y^2+y+1-(y-1)^2=3y$, le pgcd de $y-1$ et y^2+y+1 est 1 ou 3.

Ce ne peut pas être 1 car alors y^2+y+1 serait un carré ce qu'il n'est pas puisque

$$y^2<y^2+y+1<(y+1)^2.$$

Le pgcd est donc 3 et il existe $a,b\in\mathbb{N}$ tels que $x=3ab, y-1=3a^2, y^2+y+1=3b^2$. On en déduit $9a^4+9a^2+3=3b^2$ donc $3a^4+3a^2+1=b^2$.

Comme a^4+a^2 est pair, b doit être impair. En posant $b=2c+1$ on obtient alors $3a^2(a^2+1)=4c(c+1)$. Cette relation impose à a d'être pair car a^2+1 n'est pas multiple de 4.

En posant $a = 2d$ il vient $3d^2(4d^2+1) = c(c+1)$. De plus c et $c+1$ sont premiers entre eux ainsi que $3d^2$ et $4d^2+1$. En effet, si n divise $3d^2$ et $4d^2+1$ alors n divise $d^2+1 = (4d^2+1) - 3d^2$ et $3 = 3(d^2+1) - 3d^2$. Or modulo 3 on a $4d^2+1 \equiv 1$ ou 2, donc le pgcd est bien 1.

En posant $u = (3d^2) \wedge c, v = (3d^2) \wedge (c+1), w = (4d^2+1) \wedge c, t = (4d^2+1) \wedge (c+1)$, qui sont premiers entre eux deux à deux, on a

$$3d^2 = uv, 4d^2+1 = wt, c = uw, c+1 = vt.$$

• Si 3 divise u, on remplace u par $3u'$ pour obtenir

$$d^2 = u'v, 4d^2+1 = wt, c = 3u'w, c+1 = vt$$

$$d^2 = u'v, 4u'v+1 = wt, 3u'w+1 = vt \quad (*)$$

puis

$$1 = wt - 4u'v = vt - 3u'w \text{ et } u'(4v-3w) = t(w-v)$$

Comme $u' \wedge t = 1$ il existe $k \in \mathbb{Z}$ tel que $w - v = ku', 4v - 3w = kt$. On a donc $w = k(4u'+t), v = k(3u'+t)$. Ce qui prouve que $k = 1$ car $w \wedge v = 1$. On obtient donc $w = 4u'+t, v = 3u'+t$ soit $t = v - 3u', w = u' + v$ et d'après $(*)$

$$(u'+v)(v-3u') - 4u'v = 1 \text{ i.e. } -3u'^2 - 6u'v + v^2 = 1$$

Or u' et v sont premiers entre eux de produit d^2 : ce sont aussi des carrés. En remplaçant u' par u''^2 et v par v''^2 on ainsi

$$-3u''^4 - 6u''^2v''^2 + v''^4 = 1$$

D'après 4.1 on a $v'' = 1, u'' = 0$ donc $a = d = 0$ et enfin $y = 1, x = 0$

• Si 3 ne divise pas u, il divise v et on remplace v par $3v'$ pour obtenir

$$d^2 = uv', 4d^2+1 = wt, c = uw, c+1 = 3v't$$

$$d^2 = uv', 4uv'+1 = wt, uw+1 = 3v't, \quad (*)$$

puis

$$1 = wt - 4uv' = 3v't - uw \text{ et } u(4v'-w) = t(w-3v').$$

Comme $u \wedge t = 1$ il existe $k \in \mathbb{Z}$ tel que $w - 3v' = ku, 4v' - w = kt$. On a donc $w = k(4u+3t), v' = k(u+t)$. Ce qui prouve que $k = 1$ car $w \wedge v' = 1$. On obtient donc $w = 4u+3t, v' = u+t$ soit $t = v' - u, w = u + 3v'$ et d'après $(*)$

$$(u+3v')(v'-u) - 4uv' = 1 \text{ i.e. } -u^2 - 6uv' + 3v'^2 = 1.$$

Or u et v' sont premiers entre eux de produit d^2 : ce sont aussi des carrés. En remplaçant u par u''^2 et v' par v''^2 on ainsi

$$-u''^4 - 6u''^2v''^2 + 3v''^4 = 1$$

qu'on peut écrire

$$-(u''^2 + 3v''^2)^2 + 12v''^4 = 1.$$

ce qui est absurde car -1 n'est pas un carré modulo 4. Ainsi ce cas ne se produit pas et la preuve est achevée.