Journal de Théorie des Nombres
de Bordeaux **14** (2002), 629–646

Résultats élémentaires sur certaines équations diophantiennes

par Pierre SAMUEL

Résumé. Dans des travaux profonds, W. Ljunggren a montré que, pour $a > 0$ donné, les équations diophantiennes $x^4 - ay^2 = 1$ et $x^2 - ay^4 = 1$ ont au plus 1 ou 2 solutions non triviales. Par des méthodes élémentaires, je réponds ici à la question : pour quelles valeurs de a, premières ou analogues, ont-elles des solutions non-triviales ?

Abstract. Deep theorems of W. Ljunggren have shown that, for given $a > 0$, the diophantine equations $x^4 - ay^2 = 1$ and $x^2 - ay^4 = 1$, have at most 1 or 2 non trivial solutions. By elementary methods, I give here an answer to the following question : for which values of a, prime or related, do these equations have non trivial solutions ?

Il s'agit essentiellement des équations $x^4 - ay^2 = 1$ et $x^2 - ay^4 = 1$. Dans le cas où l'entier a (sans facteur carré) donné est premier ou double d'un nombre premier, on arrive à des résultats par des méthodes forts élémentaires, les seules à la portée d'un octogénaire qui n'a travaillé que dans d'autres secteurs (Géométrie Algébrique, Algèbre Commutative) mais qui, sur ses vieux jours, s'est pris de passion pour les équations diophantiennes.

D'après un célèbre théorème de Thue–Siegel–Roth, ces équations n'ont qu'un nombre fini de solutions entières. Mais combien ? et pour quelles valeurs de $a \neq 0$ (en excluant la solution triviale $(1, 0)$).

Un rappel sur l'équation $x^2 - ay^2 = 1$ sera utile. Dire que (x, y) en est une solution en entiers positifs signifie que $x + y\sqrt{a}$ est un élément de norme 1 de l'anneau $A = \mathbf{Z} + \mathbf{Z}\sqrt{a}$. Par le théorème des unités, ceux-ci sont les puissances du plus petit d'entre eux ; les solutions (x_n, y_n) de l'équation sont donc définies par $x_n + y_n\sqrt{a} = (x_1 + y_1\sqrt{a})^n$ et nous dirons que n est l'exposant de cette solution. On a $x_2 = 2x_1^2 - 1$, $y_2 = 2x_1y_1$ et l'on voit facilement que les x_n satisfont à la relation de récurrence $x_{n+1} = 2x_1x_n - x_{n-1}$; même formule pour les y_n et pour les solutions (w_n, z_n) d'équations de la forme $w^2 - az^2 = b$.

Manuscrit reçu le 17 novembre 2000.

Si une telle équation a une solution, on en obtient une infinité d'autres par multiplication par les $(x_1 + y_1\sqrt{a})^n$ et on montre qu'il n'y a qu'un nombre fini de telles familles de solutions. Il n'est pas difficile d'écrire un système de conditions nécessaires pour que $w^2 - az^2 = b$ ait des solutions, mais elles veulent dire que cette équation a des solutions en entiers p-adiques pour tout nombre premier p ; ainsi il arrive que le second nombre b, faute d'être représenté par la forme "norme" du premier membre, l'est par une forme quadratique qui lui est rationnellement équivalente, c'est-à-dire qui appartient au même "genre".

Dire que $x^4 - ay^2 = 1$ (ou $x^2 - ay^4 = 1$) a une solution veut dire qu'un x_n (ou y_n) est un carré, ce qui est un cas particulier de la recherche des carrés dans des suites récurrentes (suite de Fibonacci, de Lucas, de Pell, ...) qui a fait l'objet de nombreux articles récents.

Le pionnier de ces recherches a été le mathématicien norvégien W. Ljunggren qui, par des calculs compliqués sur les unités de certains corps biquadratiques, a montré que, pour a donné, nos équations ont au plus deux solutions (leur coexistence n'ayant lieu que pour un nombre fini de valeurs de a) (cf. [3], [6]). Ces résultats ont été précisés dans pas mal d'articles, dont un de J. H. E. Cohn (cf. [2]) qui montre que les solutions de $x^4 - ay^2 = 1$ sont nécessairement d'exposants 1 ou 2, les deux solutions ne coexistant que pour $a = 1785$ (alors $x = 13$ ou $x = 239$).

Pour x donné, il y a une unique valeur de a (sans facteur carré) telle que $x^4 - ay^2 = 1$ ait une solution : c'est le nombre $a(x)$ qui est la partie sans facteur carré de $x^4 - 1$. Ainsi, à une exception près, l'application $x \mapsto a(x)$ est injective, de sorte que l'ensemble E des valeurs de a pour lesquelles $x^4 - ay^2 = 1$ a une solution (non triviale) est infini (et récursif) ; ses éléments ≤ 1000 sont 5, 6, 15, 29, 39, 145, 210, 255, 410, 455, 791, 905, 915 et 985 (cf. [2]). Pour tester si un entier a appartient à cet ensemble, il ne semble pas y avoir d'autre moyen que de calculer "l'unité fondamentale" et de voir si x_1 ou $2x_1^2 - 1$ est un carré.

Les valeurs de a pour lesquelles il y a une solution d'exposant 2 forment un sous-ensemble infini de E ; ce sont $6, 210, 1785, 60639, \ldots$

1. Quelques lemmes

Ces lemmes sont bien connus. Je les explicite en vue des références ultérieures. On note (u_n, v_n) les solutions entières (positives) de $x^2 - 2y^2 = 1$ (on a $u_n + v_n\sqrt{2} = (3 + 2\sqrt{2})^n$) et (z_j, w_j) celle de $x^2 - 2y^2 = -1$ (on a $z_j + w_j\sqrt{2} = (1 + \sqrt{2})^{2j+1}$).

Lemme 1.1. *La seule solution de* $x^4 - 2y^2 = 1$ *est* $(1, 0)$.

Il existe k tel que $x^2 = u_k$, $y = v_k$; or on montre facilement que $u_{2n} = 4v_n^2 + 1$, $u_{2n+1} = 4w_n^2 - 1$. Que k soit pair ou impair, il s'ensuit qu'on a deux carrés de différence un, x^2 et $4v_n^2$ ou $4w_n^2$ et x^2 ; par suite $x = 0$ ou 1.

Lemme 1.2. *La seule solution de* $x^2 - 2y^4 = 1$ *est* $(1,0)$.

On a $v_{2n+1} = 2z_n w_n$ où z_n et w_n sont impairs et v_{2n+1} ne peut être un carré à cause de l'exposant de 2. Si $v_{2n} = 2u_n v_n$ est un carré, u_n, impair et premier à v_n donc à $2v_n$, est un carré ; d'où $u_n = 1,\ n = 0,\ v_{2n} = 0,\ x = 1$ et $y = 0$.

Lemme 1.3. *La seule solution de* $x^4 - 2y^2 = -1$ *est* $(1,1)$.

Astuce $y^4 - x^4 = y^4 - 2y^2 + 1 = (y^2-1)^2$. Une descente (qui remonte à Fermat) montre que $y^4 - x^4 = z^2$ implique $y = x$ (utilisation du "Pythagore arithmétique", $y^2 = q^2 + r^2$, $x^2 = q^2 - r^2$, $z = 2qr$, on recommence deux fois, etc.). Donc ici $x = y = 1$.

Lemme 1.4. *Les seules solutions de* $x^2 - 2y^4 = -1$ *sont* $(1,1)$ *et* $(239,13)$.

Résultat profond, dû à W. Ljunggren (cf. [4]). Nous l'admettrons. Notons que le même résultat peut être retrouvé simplement par les méthodes modernes de combinaison de formes lineaires de logarithmes et d'arguments effectifs.

Lemme 1.5. *L'équation* $x^2 - 2(py^2)^2 = 1$ *où* p *est premier n'a que la solution triviale* $(1,0)$ *sauf pour* $p = 2$ *(resp.* $p = 3$*) où elle a aussi la solution* $(3,1)$ *(resp.* $(17,2)$*) et nulle autre.*

Lorsque $p = 2$, on cherche un v_n de la forme $2y^2$. Si $n = 2j$, on a $u_j v_j = y^2$, donc u_j est un carré, d'où $j = 0$ (Lemme 1.1), $y = 0, x = 1$. Si $n = 2j+1$, on a $z_j w_j = y^2$, les facteurs étant premiers entre eux, donc z_j est un carré et on a $z_j = w_j = 1$ (Lemme 1.3) ; d'où $y^2 = 1,\ y = 1,\ x^2 = 8 + 1 = 9,\ x = 3$.

Pour p impair, $py^2 = v_n$ implique que y est pair car v_n est toujours pair. Ainsi v_n est multiple de 4, ce qui implique que n est pair, $n = 2j$ et qu'on a $py^2 = 2u_j v_j$. Si p divise v_j, on peut écrire $v_j = 2pv'$ (car il est pair), d'où $y^2 = 4v'u_j$; comme u_j est premier à v_j, donc à v', on en déduit que c'est un carré, d'où $u_j = 1,\ j = 0,\ v_j = 0,\ y = 0$ et $x = 1$. Si p divise u_j, on écrit $u_j = pu',\ v_j = 2v'$, d'où $y^2 = 4u'v'$; ainsi v' est un carré r^2 et on a $v_j = 2r^2$, d'où la relation $u_j^2 - 2(2r^2)^2 = 1$. Par le cas $p = 2$, on a soit $(u_j, r) = (1,0)$, soit $(u_j, r) = (3,1)$. Dans le premier cas, on obtient $v' = 0$, $y = 0$ et $x = 1$. Dans le second, on trouve $u_j = 3,\ p = 3,\ v_j = 2,\ 3y^2 = 2u_j v_j = 12,\ y^2 = 4,\ y = 2$; alors l'équation, qui s'écrit $x^2 - 18y^4 = 1$, donne $x^2 = 18 \cdot 16 + 1 = 288 + 1 = 289 = 17^2$ (miracle ?).

2. L'équation $x^4 - ay^2 = 1$ dans le cas premier

Théorème 2.1. *Si* a *est premier impair ou double d'un nombre premier impair, l'équation* $x^4 - ay^2 = 1$ *n'a que la solution triviale* $(1,0)$ *excepté pour* $a = 5$ *(resp.* $29,\ 6$*) où elle a aussi la solution* $(3,4)$ *(resp.* $(99,1820)$, $(7,20)$*) et nulle autre.*

Prenons d'abord a premier impair. L'équation s'écrit $ay^2 = (x^2-1)(x^2+1)$. Si x est pair, ces facteurs sont premiers entre eux et, comme a divise l'un d'eux, l'autre est un carré ; d'où deux entiers consécutifs qui sont des carrés et la solution triviale.

Donc x est impair, on a $\operatorname{pgcd}(x^2-1, x^2+1) = 2$ avec x^2-1 multiple de 8 et x^2+1 juste pair. Deux cas selon que a divise x^2-1 ou x^2+1. S'il divise x^2-1, on peut écrire $x^2-1 = 8aq'$, $x^2+1 = 2r'$ (r' impair), d'où $16q'r' = y^2$ de sorte que q' et r' sont des carrés q^2 et r^2. Ainsi $x^2-1 = 8aq^2$, $x^2+1 = 2r^2$ et $y = 4qr$. Comme $x^2 - 2r^2 = -1$, x est l'un des z_j et on a $r = w_j$ (notation du §1). On a $r^2 - 4aq^2 = 1$ d'où $4aq^2 = w_j^2 - 1$ qui, par un petit calcul, vaut $v_j(3v_j + 2u_j) = v_j v_{j+1}$. Or les v_j sont pairs, $v_j = 2v'_j$ et, comme $v'_{j+1} = 3v'_j + u_j$, il est premier à v'_j. Or $aq^2 = v'_j v'_{j+1}$, de sorte que a divise l'un des deux facteurs et que l'autre est un carré. Or (Lemme 1.5, cas $p = 2$), v'_j n'est un carré que si $j = 0$ (donnant la solution triviale), ou si $v'_j = 1$, $v_j = 2, j = 1$, $v_{j+1} = v_2 = 12$, $aq^2 = 6$, impossible car a est impair.

Passons au cas où a (premier) divise x^2+1. Comme ci-dessus, on peut écrire $x^2-1 = 2q^2$, $x^2+1 = 2ar^2$, d'où $y = 2qr$, $ar^2 - q^2 = 1$ et $x^2 - 2q^2 = 1$. Ainsi q est l'un des v_n et un petit calcul montre que $ar^2 = v_n^2 + 1$ vaut $w_{n-1}w_n$. Comme $w_n = 3w_{n-1} + 2z_{n-1}$ et que w_{n-1}, impair, est premier à z_{n-1}, on voit que w_{n-1} et w_n sont premiers entre eux. Comme a divise l'un d'eux, l'autre est un carré ce qui, par le lemme de Ljunggren (Lemme 1.4), donne 3 possibilités :

- $n = 1$, $w_{n-1} = w_0 = 1$, $w_n = w_1 = 5$, $ar^2 = 5$, $a = 5$, $r = 1$, $q = v_1 = 2$, $y = 2qr = 4$ et $x = 3$.
- $n = 3$, $w_3 = 169 = 13^2$, $w_2 = 29$, $a = 29$, $r = 13$, $q = v_3 = 70$, $x = u_3 = 99$ et $y = 2qr = 1820$.
- Si $n = 4$, c'est $w_{n-1} = w_3$ qui est le carré et $w_4 = 985$ est de la forme as^2 ; mais $985 = 5 \cdot 197$ est sans facteur carré, d'où $s = 1$ et $a = 985$ non premier (on a alors $r = 13$, $q = v_4 = 408$, $x = u_4 = 577$ et $y = 2qr = 10608$).

Enfin le cas $a = 2p$, p premier impair. La relation $(x^2-1)(x^2+1) = 2py^2$ montre que x est impair (et donc y pair). Si p divise x^2+1, on peut donc poser $x^2-1 = 4q'$, $x^2+1 = 2pr'$, d'où $4q'r' = y^2$ de sorte que q' et r' sont des carrés q^2 et r^2 et qu'on a $x^2 - 4q^2 = 1$, soit $(x+2q)(x-2q) = 1$, impossible sauf si $x = 1$, $q = 0$, $y = 0$, solution triviale. Donc p divise x^2-1 et on peut écrire $x^2 - 1 = 4pq^2$, $x^2 + 1 = 2r^2$ et $y = 2qr$. Comme $x^2 - 2r^2 = -1$, x est l'un des z_j d'où, par un calcul facile, $4pq^2 = z_j^2 - 1 = 2v_j v_{j+1}$. Comme ci-dessus, on pose $v_j = 2v'_j$ et on note que v'_j est pair si et seulement si j est pair. Alors $pq^2 = v'_j v'_{j+1}$. Si p divise v'_j, soit $v'_j = pv''$, on a $q^2 = 2v''v'_{j+1}$; si j est pair, v'_{j+1}, impair et premier à $2v''$, est un carré d'où (Lemme 1.5) $v_{j+1} = 2$, $j = 0$, $v'_j = 0$, impossible ; si j est impair, c'est v'' qui est impair et $2v'_{j+1} = v_{j+1}$ est un carré, d'où $j+1=0$ (Lemme 1.2), impossible encore. Donc p divise v'_{j+1} soit $v'_{j+1} = pv''$ et $q^2 = 2v'_j v''$; si j est pair, v'' (impair) et $2v'_j = v_j$ sont des carrés, d'où $v_j = 0$ et la solution est triviale ; enfin si j est impair, v'_j, impair, est un carré donc (Lemme 1.5) $j=1$, $v_j = 2$, $x = z_1 = 7$, $r = w_1 = 5$, $pv'' = v'_{j+1} = v'_2 = 6$, $p = 3$ et l'équation $7^4 - 6y^2 = 1$ donne $6y^2 = 2400$, $y^2 = 400$ et $y = 20$ (obtenu aussi via $y = 2qr$).

Remarque. L'hypothèse de primalité a été utilisée de façon essentielle à au moins deux reprises dans chacun des trois cas.

Dans le cas général, les solutions avec x pair ne sont pas exclues (prendre pour a la partie sans facteur carré de x^4-1). La plus simple est $(2,1)$ pour $a=15$.

Si l'on s'intéresse, par exemple, au cas où a (composé) est impair, un facteur b de a va dans x^2-1, l'autre c dans x^2+1. On peut montrer que la décomposition $a = bc$ est uniquement déterminée par a, mais ceci ne nous avance guère.

Un cas assez favorable est celui où tous les facteurs premiers de a sont $\equiv -1$ modulo 4 car aucun ne peut diviser x^2+1, ce qui implique $c=1$. Le cas où x est pair est exclu car alors on peut écrire $x^2-1 = aq^2$, $x^2+1 = r^2$, d'où $x=0$, impossible. Donc x est impair et l'on écrit $x^2-1 = 2aq^2$, $x^2+1 = 2r^2$; d'où le système diophantien $(r^2 - aq^2 = 1,\ x^2 - 2aq^2 = 1)$ qu'on peut traiter directement dans certains cas.

Les résultats voisins suivants seront utiles dans la suite :

Théorème 2.2. *L'équation* $4x^4 - ay^2 = 1$, *où a est premier, n'a de solutions que si $a=3$ ou $a=7$: solutions* $(1,1)$ *et* $(2,3)$ *et nulles autres.*

Dans $ay^2 = (2x^2-1)(2x^2+1)$ les facteurs sont impairs et premiers entre eux. Si a divise $2x^2+1$, on peut écrire $2x^2+1 = ar^2$, $2x^2-1 = s^2$ de sorte que x est un w_j et qu'on a $ar^2 = 2w_j^2 + 1 = u_j u_{j+1}$ (calcul facile). Donc l'un des nombres u_j, u_{j+1} est un carré car u_j est premier à $u_{j+1} = 3u_j + 4v_j$. On a donc $j=0$ (Lemme 1.1), $u_j = 1$, $u_{j+1} = 3$, $a=3$, $r=1$, $s=1$, $x=1$ et $y=1$.

Si a divise $2x^2-1$, on peut écrire $2x^2-1 = as^2$, $2x^2+1 = r^2$, de sorte que x est un v_n et qu'on a $as^2 = 2v_n^2 - 1 = z_n z_{n-1}$. Ainsi a divise l'un des nombres z_n, z_{n-1} et l'autre est un carré, car ils sont premiers entre eux. Comme $n=0$ est impossible, on a $n-1=0$ (Lemme 1.3), $n=1$, $as^2 = 7$, $a=7$, $s=1$, $2x^2 = 8$, $x=2$ et $y=3$.

Corollaire 2.3. *Pour a premier, l'équation $x^4 - ay^2 = 4$ n'a de solution que si $a=3$ ou $a=7$: solutions* $(2,2)$ *et* $(4,6)$ *et nulles autres.*

Si $a=2$, x doit être pair et donc $2y^2$ multiple de 4 ; ainsi y est pair et le premier membre est multiple de 8, impossible.

Donc a est impair. Si x est impair, on écrit $ay^2 = (x^2+2)(x^2-2)$ et l'on voit que les facteurs sont impairs et premiers entre eux (leur différence est 4). L'un d'eux est donc multiple de a et l'autre est un carré. On a alors deux carrés dont la différence est 2, impossible.

Donc x est pair, $x = 2x'$ et y l'est aussi, $y = 2y'$. Alors $4x'^4 - ay'^2 = 1$ et on applique le Théorème 2.2.

Enfin un analogue du Lemme 1.5 :

Théorème 2.4. *Pour p premier impair, l'équation $x^2 - 8p^2y^4 = 1$ n'a que la solution triviale $(1, 0)$, sauf pour $p = 239$ où elle a aussi la solution $(114243, 13)$ et nulle autre.*

En effet, $2py^2$ est un v_n. Si $n = 2j$, on a $py^2 = u_jv_j$, l'un des facteurs est un carré, on a $j = 0$ (Lemmes 1.1 et 1.2) et la solution est triviale. Si $n = 2j+1$, on a $py^2 = z_jw_j$. Le cas $j = 0$ est exclu car alors $py^2 = 1$. Par les Lemmes 1.3 et 1.4, il ne reste que $j = 3$ où $w_3 = 13^2$ et $z_3 = 239$; alors $p = 239$, $y = 13$ et $x = u_7 = 114243$ $(= 3 \cdot 113 \cdot 337)$.

3. Autre approche via une analyse des unités

Lemme 3.1. *Soient p un nombre premier impair et x, y des entiers strictement positifs tels que $x^2 - py^2 = 1$. On pose $U = x + y\sqrt{p}$ $(N(U) = 1)$. Alors :*

(a) *Si x est pair, il existe un élément $V = u + v\sqrt{p}$ tel que $u^2 - pv^2 = \pm 2$, $v^2 = 2U$, $y = uv$ et $u^2 = x \pm 1$. Alors $p \equiv -1$ modulo 4.*

(b) *Si x est impair et si p divise $x+1$, il existe un élément $V = 2u + v\sqrt{p}$ de norme -1 tel que $V^2 = U$. Alors $p \equiv 1$ modulo 4.*

(c) *Si x est impair et si p divise $x-1$, il existe un élément $V = u' + v'\sqrt{p}$ de norme 1 telque $V^2 = U$.*

Ecrivons $(x+1)(x-1) = py^2$. Si x est pair, $x+1$ et $x-1$ sont premiers entre eux et p divise l'un d'eux. Si c'est $x+1$, on peut écrire $x+1 = pv^2$, $x-1 = u^2$, $y = uv$; alors $u^2 - pv^2 = -2$. Si c'est $x-1$, on écrit $x-1 = pv^2$, $x+1 = u^2$, $y = uv$; alors $u^2 - pv^2 = 2$. On a $-py^2 \equiv 1$ modulo 4, d'où $p \equiv -1$ modulo 4 ; d'où (a).

Si x est impair, l'hypothèse donne $1 - py^2 \equiv 1$ modulo 8, $py^2 \equiv 0$ modulo 8 et y doit être multiple de 4, $y = 4y'$. Comme $\mathrm{pgcd}(x+1, x-1) = 2$, la relation $(x+1)(x-1) = 16py'^2$ montre que l'un des deux nombres $x+1$, $x-1$ est "juste pair", l'autre étant multiple de 8. D'où 4 cas, suivant la répartition des facteurs p et 8 entre $x+1$ et $x-1$:

(1) $x+1 = 8pv^2$, $x-1 = 2u^2$ (u impair). Alors $4pv^2 - u^2 = 1$, impossible modulo 4.

(2) $x+1 = 2pv^2$, $x-1 = 8u^2$, d'où $4u^2 - pv^2 = -1$; alors $V = 2u + v\sqrt{p}$ est de norme -1 et on a $x = 4u^2 + pv^2$, $y = 4uv$, d'où $V^2 = U$. On voit que $p \equiv 1$ modulo 4.

(3) $x+1=2u^2$, $x-1=8pv^2$, d'où $u^2-p(2v)^2=1$; alors $V=u+2v\sqrt{p}$ est de norme 1 et on $V^2=U$. On ne voit pas de contrainte sur p.

(4) $x+1=8u^2$, $x-1=2pv^2$, d'où $4u^2-pv^2=1$; alors $V=2u+v\sqrt{p}$ est de norme 1 et on a $V^2=U$.

Ainsi (2) donne le (b) de l'énoncé, (3) ou (4) le (c).

Remarque. Si $p\equiv 1$ modulo 4 et si l'on prend pour U la plus petite unité de norme 1, (a) et (c) sont exclus d'où, par (b), l'existence d'une unité de norme -1, ce qui est sûrement connu. Mais pour a composé, et même si -1 est un carré modulo a, il peut n'exister aucune unité de norme -1 ; par exemple, pour $a=221=13\cdot 17$, on a $U=1165+112\sqrt{221}$ et $U=(u+v\sqrt{221})^2$ avec $u^2-221v^2=-1$ est impossible car, sinon, $1165=2u^2+1$ et $u^2=582$ qui n'est visiblement pas un carré.

Théorème 3.2. *Pour p premier $\equiv -1$ modulo 4, l'équation $x^4-py^2=1$ n'a pas de solution non triviale.*

Pour une solution d'exposant impair, le (c) du lemme est exclu, on est dans le cas (a) et on a $x^2\pm 1=u^2$, d'où deux entiers consécutifs qui sont des carrés et la solution triviale.

Pour une solution d'exposant "juste pair", soit $2j$ avec j impair, on note $x'+y'\sqrt{p}$ l'élément d'exposant j. Alors $x^2=2x'^2-1$. Mais x' est pair par (a) et c'est impossible modulo 4.

Enfin, si l'exposant est multiple de 4, c'est encore impossible à cause du lemme suivant, dû à J. H. E. Cohn (cf. [1]) :

Lemme 3.3. *Pour a quelconque, l'équation $x^4-ay^2=1$ n'a aucune solution (non triviale) d'exposant multiple de 4. Autrement dit l'équation $8x^4-8x^2+1=t^2$ n'a que la solution $(x,t)=(0,1)$.*

En effet $(x+y\sqrt{a})^4=8x^4-8x^2+1+4xy(2x^2-1)\sqrt{a}$ (utiliser $ay^2=x^4-1$). De $8x^4-8x^2+1=t^2$, on tire $t^2+8x^4=16x^4-8x^2+1=(4x^2-1)^2$, d'où $8x^4=(4x^2-1+t)(4x^2-1-t)$. Comme t est premier à x, le pgcd des deux facteurs, qui divise $2t$ où t est impair, et $8x^4$, ne peut pas être que 2 ; l'un des deux facteurs est donc multiple de 4. En posant, par exemple, $4x^2-1+t=4q'$ et $4x^2-1-t=2r'$, $x^4=q'r'$ montre que q' et r' sont des bicarrés q^4 et r^4 ; alors $x=qr$, $4x^2-1=2q^4+r^4$; de même dans l'autre cas. On a donc $2q^4+r^4=4q^2r^2-1$, d'où $r^4-2(r^2-q^2)^2=1$. Par le Lemme 1.1, on en déduit $r=1$, $q^2-r^2=0$, $q=1$, d'où $x=1$ et $t=1$ et la solution triviale.

Remarque. Pour $p\equiv -1$ modulo 4, cette démonstration, qui n'utilise que les Lemmes 1.1 et 3.1, est plus rapide que celle donnée dans le Théorème 2.1.

Pour $p\equiv 1$ modulo 4, les solutions d'exposant multiple de 4 sont éliminées par le lemme de Cohn. Pour celles d'exposant $2j$, j impair, on note

$x'+y'\sqrt{p}$ l'unité d'exposant j qui, par le Lemme 3.1 est le carré $(u+v\sqrt{p})^2$ d'une unité de norme -1 ; d'où $x'=2u^2+1$ et $x^2=2x'^2-1=8u^4+8u^2+1$, une équation qu'on traite comme celle du lemme de Cohn et qui n'a que la solution $x=1,\ u=0$. Mais, pour une solution d'exposant impair, on tombe sur les relations $x^2=2u^2+1,\ u^2-pv^2=-1$, que je ne sais traiter que par la méthode du Théorème 2.1.

Passons aux doubles de nombres premiers :

Lemme 3.4. *Soient p un nombre premier impair et $x,\ y$ deux entiers strictement positifs tels que $x^2-2py^2=1$. On pose $U=x+y\sqrt{2p}$. Alors :*

(a) *Si $4p$ divise $x+1$ (resp. $x-1$), il existe un élément $V=r+q\sqrt{2p}$ de norme -1 (resp. $+1$) tel que $V^2=U$.*

(b) *Si 4 divise $x+1$ et p divise $x-1$ (resp. si 4 divise $x-1$ et p divise $x+1$), il existe un élément $V=2r+q\sqrt{2p}$ de norme 2 (resp. -2) tel que $V^2=2U$. Alors q est impair et on a $p\equiv -1$ modulo 8 si r pair et $p\equiv 1$ modulo 8 si r est impair (resp. $p\equiv 1$ modulo 8 si r est pair et $p\equiv 3$ modulo 8 si r est impair).*

En effet x est impair donc (voir modulo 8) y est pair, $y=2y'$ et on écrit $8py'^2=(x+1)(x-1)$. On répartit les facteurs 4 et p entre $x+1$ et $x-1$, d'où 4 cas. Le reste est un “âne qui trotte” comme dans le Lemme 3.1.

Remarque. Si $p\equiv 5$ modulo 8, le (b) de l'énoncé est exclu. Donc, en prenant U d'exposant 1, on voit qu'il existe une unité $V=r+q\sqrt{2p}$ de norme -1. Par contre si $p\equiv 1$ modulo 8, l'existence d'unités de norme -1 dépend de p : il y en a pour $p=41,\ 113,\ 137$; il n'y en a pas pour $p=17,\ 73,\ 89,\ 97$.

Théorème 3.5. *Si p est premier impair, l'équation $z^4-2py^2=1$ n'a pas de solution d'exposant impair. Sa seule solution non triviale a lieu pour $p=3$, $2p=6$ et est $(7,20)$ (d'exposant 2).*

Posons $U=z^2+y\sqrt{2p}$. Si son exposant est impair, on a soit $U=(r+q\sqrt{2p})^2$ avec $r^2-2pq^2=-1$, soit $2U=(2r+q\sqrt{2p})^2$ avec $4r^2-2pq^2=\pm 2$. Dans le premier cas, on trouve $z^2=2r^2+1=4pq^2-1$, impossible modulo 4. Dans le second, on trouve $z^2=4r^2\pm 1$, impossible encore.

Le cas d'un exposant multiple de 4 étant exclu par le lemme de Cohn, reste celui d'un exposant $2j$ avec j impair. Soit $x'+y'\sqrt{2p}$ l'unité d'exposant j. On a alors $z^2=2x'^2-1$. D'après le calcul ci-dessus, on a soit $x'=2r^2+1$, soit $x'=4r^2\pm 1$.

Si $x'=2r^2+1$ on a $z^2=8r^4+8r^2+1$, d'où (cf. lemme de Cohn) $8r^4=(4r^2+1+z)(4r^2+1-z)$ et des entiers a,b tels que $4r^2+1=a^4+2b^4$ et $r=ab$. D'où $(a^2-2b^2)^2-2b^4=1$ qui implique $b=0,\ a=1$ (Lemme 1.2) $r=0$ et $z=1$, solution triviale.

Si $x' = 4r^2 - 1$, on a $z^2 = 32r^4 - 16r^2 + 1$. Comme ci-dessus, il y a des entiers a et b tels que $8r^2 - 1 = 8a^4 + b^4$, impossible modulo 4.

Enfin, si $x' = 4r^2 + 1$, on trouve de même $8r^2 + 1 = 8a^4 + b^4$ avec $r = ab$. D'où $(b^2 - 4a^2)^2 - 8a^4 = 1$ ce qui, par le Lemme 1.5, donne l'unique solution non triviale $a = 1$, $b^2 - 4a^2 = \pm 3$; le signe $+$ donne $b^2 = 7$, impossible ; avec $-$, on trouve $b = 1$, $r = 1$, $x' = 5$, $z^2 = 2 \cdot 5^2 - 1 = 49$, $z = 7$, $2py^2 = z^4 - 1 = 2400 = 6 \cdot 20^2$ d'où $2p = 6$ et $y = 20$.

Cette méthode n'est pas plus simple que celle du Théorème 2.1.

Complément 3.6. Dans les démonstrations des Théorèmes 3.2 et 3.5 nous avons uniquement utilisé l'existence d'éléments V de norme ± 2 (resp. de norme -1) tels que $V^2 = 2U$ (resp. $V^2 = U$).

La simple existence de $V = u + v\sqrt{a}$ tel que $u^2 - av^2 = \pm 2$ montre qu'on a $V^2 = u^2 + av^2 + 2uv\sqrt{a} = 2u^2 \pm 2 + 2uv\sqrt{a}$ et que la norme de $U = u^2 \pm 1 + uv\sqrt{a}$ vaut $(u^2 \pm 1)^2 - u^2v^2a = (u^2 \pm 1)^2 - u^2(u^2 \pm 2) = 1$. L'unité U est d'exposant impair car, sinon, il y aurait une unité U' telle que $U = U'^2$, d'où $V^2 = 2U'^2$, $(V \cdot U'^{-1})^2 = 2$ d'où des entiers r, s tels que $(r + s\sqrt{a})^2 = 2$; ainsi $r^2 + as^2 = 2$, $rs = 0$, ce qui n'est possible que si $r = 0$, $s = 1$, $a = 2$, un cas qui, traité dans les lemmes du §1, sera désormais exclu. En notant U_0 la plus petite unité de norme 1, on a ainsi $U = U_0^{2j+1}$, d'où $(VU_0^{-j})^2 = 2U_0$; il y a donc un élément V_0 de norme ± 2 (et à coefficients > 0 moyennant un changement de signe) tel que $V_0^2 = 2U_0$. De même pour toute puissance impaire de U.

De même, s'il existe une unité de norme -1, soit V, V^2 est une unité U de norme 1 d'exposant impair ; alors U_0 et toutes les unités d'exposant impair sont des carrés d'unités de normes -1.

Soit $U = x + y\sqrt{a}$ une telle unité d'exposant impair et soit $V = u + v\sqrt{a}$ l'élément tel que $V^2 = 2U$ (resp. $V^2 = U$) ; Le tableau suivant des parités sera utile dans la suite :

$N(V) = \pm 2$, a impair ($\equiv -1$ modulo 4) : x pair, y impair, u impair, v impair.
$N(V) = \pm 2$, $a = 2a'$ ($a' \equiv -1$ modulo 4) : x impair, y pair, u pair, v impair.
$N(V) = -1$, a impair ($\equiv 1$ modulo 4) : x impair, y pair, u pair, v impair.
$N(V) = -1$, $a = 2a'$ ($a' \equiv 1$ modulo 4) : x impair, y pair, u impair, v impair.

(Démonstrations faciles, où l'on commence par u et v.)

4. Intermède : éléments et équations satellites

Soient a sans facteur carré et $U = x + y\sqrt{a}$ la plus petite unité de norme 1. On vient de constater, dans certains cas, l'existence d'un élément V tel que

V^2 soit proportionnel à U. C'est général. En effet, en posant $V = u + v\sqrt{a}$, écrire $V^2 = kU$ se traduit par $u^2 + av^2 = kx$, $2uv = ky$, d'où l'équation $yu^2 - 2xuv + ayv^2 = 0$, dont le discriminant réduit est $x^2 - ay^2 = 1$ et qui a les solutions $u/v = (x+1)/y$ et $u/v = (x-1)/y$. On voit aussi qu'on a :

$$\text{(a)} \qquad (x+1+y\sqrt{a})^2 = 2(x+1)U, \quad (x-1+y\sqrt{a})^2 = 2(x-1)U$$
$$N(x+1+y\sqrt{a}) = 2(x+1), \quad N(x-1+y\sqrt{a}) = -2(x-1).$$

On simplifie les éléments obtenus par $g = \mathrm{pgcd}(x+1, y)$ et $g' = \mathrm{pgcd}(x-1, y)$, d'où deux éléments $V = u+v\sqrt{a}$ et $V' = u'+v'\sqrt{a}$, qu'on peut appeler les "satellites" de l'unité U.

De $(x+1)(x-1) = ay^2$, on déduit $gu \cdot g'u' = a \cdot gv \cdot g'v'$, d'où $uu' = avv'$. Comme u est premier à v et u' à v', u divise av' et on pose $av' = b'u$; de même $av = bu'$. Ainsi $bb'uu' = a^2vv' = auu'$ et $bb' = a$; donc $u = bv'$ et $u' = b'v$. Puis il y a deux cas suivant la parité de x :

1) Si x est pair, $x+1$ et $x-1$ sont impairs et premiers entre eux, donc g et g' aussi. De $y = gv = g'v'$, on déduit que g divise v', $v' = kg$ d'où $v = kg'$. Alors u vaut $bv' = bkg$. Comme $v = kg'$ est premier à u, on en déduit $k = 1$, $v = g'$, $u = bg$, $v' = g$, $u' = b'g'$. Comme $x+1 = gu = bg^2$ et $x-1 = g'u' = {g'}^2b'$, on déduit de (a) qu'on a :

$$\text{(b)} \quad N(V) = 2b,\ V^2 = 2bU,\ N(V') = -2b',\ {V'}^2 = 2b'U \quad (\text{avec } a = bb').$$

2) Si x est impair, $x+1$ et $x-1$ ont 2 pour pgcd, donc g et g' aussi, soit $g = 2g_1$, $g' = 2g'_1$. Comme ci-dessus, on écrit $v' = kg_1$, $v = kg'_1$, $u = bkg_1$ et $k = 1$. Ainsi $v = g'_1$, $v' = g_1$, $u = bg_1$, $u' = b'g'_1$. De $2(x+1) = 2gu = 4g_1u = g^2b$ et de $2(x-1) = {g'}^2b'$, on déduit de (a) qu'on a :

$$\text{(b')} \qquad N(V) = b,\ V^2 = bU,\ N(V') = -b',\ {V'}^2 = b'U.$$

En changeant un peu les notations, considérons les équations

$$\text{(c)} \qquad u^2 - av^2 = b,\ {u'}^2 - a{v'}^2 = -b' \quad (\text{pour } x = x_1 \text{ impair}),$$

$$\text{(c')} \qquad u^2 - av^2 = 2b,\ {u'}^2 - a{v'}^2 = -2b' \quad (\text{si } x = x_1 \text{ pair}).$$

On peut les appeler les "satellites" de l'équation $x^2 - ay^2 = 1$. Leurs solutions sont données par les VU^n et les $V'U^n$. Elles sont équivalentes car, dans une solution de la première, b divise u^2 et donc u car il est sans facteur carré ; en posant $u = bw$, on obtient $bw^2 - b'v^2 = 1$ (resp. $= 2$), d'où $aw^2 - (b'v)^2 = b'$ (resp. $2b'$) et $(b'v', w)$ est solution de la seconde. Notons les relations :

$$\text{(d)} \qquad bw^2 - b'v^2 = 1 \text{ si } x \text{ est impair} ; \quad bw^2 - b'v^2 = 2 \text{ si } x \text{ est pair}.$$

La relation $(VU^n)^2 = bU^{2n+1}$ (resp. $2bU^{2n+1}$) donne $bx_{2n+1} = u^2 + av^2 = 2u^2 - b = 2b^2w^2 - b$, en posant $u_n = u$, $v_n = v$ (resp. $2bx_{2n+1} = 2b^2w^2 - 2b$) et $by_{2n+1} = 2uv = 2bwv$ (resp. $2by_{2n+1} = 2uv = 2bwv$). On a donc :

(e) $\quad x_{2n+1} = 2bw^2 - 1 = 2b'v^2 + 1$ et $y = 2wv$ si x est impair ;

(e') $\quad x_{2n+1} = bw^2 - 1 = b'v^2 + 1$ et $y = wv$ si x est pair.

Dans les bons cas où a est premier ou double d'un nombre premier, les résultats de parité donnés à la fin du §3 se précisent comme suit (avec les présentes notations, on les applique à $u' = b'v$ et $v' = w$ en cas de norme < 0) :

- $N(V) = -1$, a impair $\equiv 1$ modulo 4, x impair, $b' = 1$, v pair, w impair.
- $N(V) = -1$, $a = 2a'$, $a' \equiv 1$ modulo 4, x impair, $b' = 1$, v impair, w impair.
- $N(V) = 2$ ou $N(V') = -2$, $a \equiv -1$ modulo 4, x pair, v impair, w impair.
- $N(V) = 2$, $a = 2a'$, $a' \equiv -1$ modulo 4, $b = 2$, x impair, v impair, w pair, alors $a' \equiv -1$ modulo 8 (examiner (d) modulo 8).
- $N(V) = -2$, $a = 2a'$, $a' \equiv -1$ modulo 4 : x impair, v impair, w impair ; alors $a' \equiv 3$ modulo 8 (idem).

Remarque. Étant donné un nombre premier p, notons $k(p)$ l'ordre modulo p de l'unité fondamentale U (c'est-à-dire l'ordre de l'image de U dans le groupe multiplicatif $(A/Ap)^*$ où $A = \mathbf{Z} + \mathbf{Z}\sqrt{a}$). On montre que cet ordre divise $p+1$ si p est inerte, et $p-1$ si p est décomposé. Si p impair est ramifié (c'est-à-dire s'il divise a), on a $k(p) = p$ si $x_1 \equiv 1$ modulo p et $k(p) = 2p$ si $x_1 \equiv -1$ modulo p.

Notons (x_n, y_n), (u_n, v_n) les solutions de $x^2 - ay^2 = 1$ et de sa première satellite. Pour p premier non ramifié, on peut montrer :

- p divise un x_n ssi $k(p)$ est multiple de 4 ;
- p divise l'un des u_j ssi $k(p)$ est impair ;
- p divise l'un des v_j ssi $k(p)$ est de la forme $2k'$ avec k' impair.

Donc, les diviseurs premiers (non ramifiés) des x_n, des u_j et des v_j forment 3 ensembles disjoints.

5. Aperçus élémentaires sur l'équations $x^2 - az^4 = 1$

Nous noterons $U = x_1 + y_1\sqrt{a}$ la plus petite unité de norme 1 contenue dans $\mathbf{Z} + \mathbf{Z}\sqrt{a}$ (a sans facteur carré). Les solutions de $x^2 - ay^2 = 1$ sont alors les (x_n, y_n) définis par $x_n + y_n\sqrt{a} = U^n$.

Si x_1 est pair, y_1 est impair et on a $a \equiv -1$ modulo 4. Alors tous les x_{2n+1} sont pairs, avec la même puissance 2^k de 2 que x_1.

Utiliser $x_3 = x_1(4x_1^2 - 3)$ puis la récurrence $x_{2j+3} = 2x_2x_{2j+1} - x_{2j-1}$. Inversement les x_{2n+1} sont pairs si $a \equiv -1$ modulo 4 et s'il existe un satellite V de norme ± 2, en particulier si a est premier (Lemme 3.1 et §4). Comme $x_{2n} = 2x_n^2 - 1$, les x_{2n} sont toujours impairs. Si $a \equiv 1$ ou 2 modulo 4, tous les x_n sont impairs et alors y_n est pair (opérer modulo 8).

Théorème 5.1. *L'équation* $x^2 - az^4 = 1$ *n'a de solution (non triviale) d'exposant multiple de* 4 *que si* $a = 1785$. *Elle a alors la solution* $(169, 2)$ *d'exposant* 1*, la solution* $(6525617281, 12428)$ *d'exposant* 4 *et nulle autre.*

En effet, on a $y_{4n} = 2x_{2n}y_{2n} = 4x_{2n}x_ny_n$, les trois facteurs étant premiers entre eux deux-à-deux. Donc, si y_{4n} est un carré, x_n est un carré s^2 et $x_{2n} = 2x_n^2 - 1$ en est un autre, t^2. Par un théorème de Ljunggren (Lemme 1.4), cela implique soit $(s,t) = (1,1)$ (alors $x_n = 1$, $n = 0$, $y_n = 0$, solution triviale) soit $(s,t) = (13, 239)$. Dans ce cas, de $x_n = 169$ $(= 13^2)$, on déduit $ay_n^2 = 169^2 - 1 = 4^2 \cdot 1785$, d'où $a = 1785$ car $1785 = 3 \cdot 5 \cdot 7 \cdot 17$ est sans facteur carré, et (miracle ?) $y_n = 4$ est un carré. On a évidemment $n = 1$. Alors $y_4 = 4t^2s^2 \cdot 4$ est le carré de $4st = 4 \cdot 13 \cdot 239 = 12428$, et l'équation donne la valeur de x_4.

Théorème 5.2. *S'il existe un satellite* V *de norme* -1 *(resp.* ± 2*) tel que* $V^2 = U$ *(resp.* $V^2 = 2U$*), en particulier si* a *est premier ou le double d'un nombre premier, l'équation* $x^2 - az^4 = 1$ *n'a de solution (non triviale) d'exposant "juste pair"* $n = 2(2j+1)$ *que si* $a = 3$ *; elle a alors la solution* $(7, 2)$ *d'exposant* 2 *et la solution* $(2, 1)$ *d'exposant* 1.

En effet, soit $x' + y'\sqrt{a}$ l'unité d'exposant $2j + 1$ telle que $x + z^2\sqrt{a} = (x' + y'\sqrt{a})^2$. Alors $x = 2x'^2 - 1$ et $z^2 = 2x'y'$. D'où 2 cas :

- Si x_1 et donc x', est impair, alors x' est un carré q^2 et y' est de la forme $y' = 2r^2$. On a donc $q^4 - 4ar^4 = 1$. Notons $u + v\sqrt{a}$ le satellite de norme positive attaché à $x' + y'\sqrt{a}$ (cf. §4). Avec les notations du §4 $(a = bb',\ u = bw)$, la formule $2r^2 = y' = 2wv$ montre que w et v sont des carrés s^2 et t^2. Par (d) et (e) du §4, on a donc :

$$\text{(a)} \qquad bs^4 - b't^4 = 1,\ q^2 = 2bs^4 - 1 = 2b't^4 + 1,\ r = st,\ q^2 = bs^4 + b't^4.$$

En cas d'unité de norme -1, on a $b' = 1$ d'où $q^2 = 2t^4 + 1$ et par le Lemme 1.2, $q = 1,\ t = 0,\ v = 0,\ x' = 1,\ z = 0$, solution triviale.

En cas de satellite de norme 2 ou -2, on a soit $b = 2$ soit $b' = 2$. Si $b = 2$, on trouve $q^2 = 4s^4 - 1$, $(2s^2 - q)(2s^2 + q) = 1$, impossible. Si $b' = 2$, $q^2 = 4t^4 + 1$ est tout aussi impossible.

- Passons au cas où x_1, et donc x', est pair (ce qui implique $a \equiv -1$ modulo 4 et exclut les unités de norme -1) ; c'est y' qui est un carré r^2 et x' est de la forme $2q^2$. On a ainsi $4q^4 - ar^4 = 1$. Avec les notations du §4 pour le satellite, la formule $r^2 = y' = wv$ montre que w et v sont des carrés

s^2 et t^2 et les formules (d) et (e') du §4 donnent :

(a') $\quad bs^4 - b't^4 = 2,\ 2q^2 = bs^4 - 1 = b't^4 + 1,\ r = st,\ bs^4 + b't^4 = 2q^2.$

Les satellites étant ici de normes $2b$ et $-2b'$, l'on voit que, si l'un est de norme 2 ou -2, on a soit $b = 1$, soit $b' = 1$. Si $b = 1$, $2q^2 = s^4 - 1$ donne $s = 1$, $q = 0$ par le Lemme 1.1, d'où $b't^4 + 1 = 0$ impossible. Si $b' = 1$, on a $t^4 - 2q^2 = -1$ d'où $t = q = 1$ par le Lemme 1.3, $bs^4 = 2q^2 + 1 = 3$, $b = 3,\ a = 3,\ s = 1,\ r = 1,\ y' = 1,\ x' = 2,\ z = 2$ et $x = 7$.

Complément 5.3. Examinons ce qui peut se passer si l'on ne fait pas d'hypothèse sur V.

Si x_1 est impair et si a est impair, donc aussi b et b', les relations (a) montrent que s ou t doit être pair. Si c'était s, on aurait $q^2 \equiv -1$ modulo 4, impossible. C'est donc t et comme 1 est le seul bicarré impair modulo 16, on voit qu'on a $b \equiv 1$ modulo 16.

Si a est pair, b ou b' l'est aussi. Si c'est b, on a $q^2 \equiv -1$ modulo 4 impossible. Donc c'est b', $b' = 2b''$ (b'' impair car a et b sont sans facteur carré), et $bs^4 - 2b''t^4 = 1$ montre que s est impair. Si t était impair, on aurait $b - 2b'' \equiv 1$ modulo 16 et $b + 2b'' \equiv q^2$ modulo 16 ; or les carrés impairs modulo 16 sont 1 et 9, d'où, dans le premier cas, $4b'' \equiv 0$ modulo 16 et b'' serait pair, impossible ; dans le second, on aurait $4b'' \equiv 8$ modulo 16, impossible encore. Donc t est pair et on a $b \equiv 1$ modulo 16 et $q^2 \equiv 1$ modulo 32.

On peut aussi, en utilisant $q^4 - 4ar^4 = 1$, examiner la liste des valeurs de a pour lesquelles $x^4 - ay^2 = 1$ a une solution pour voir si y peut être le double d'un carré. Sur les 58 premières (données dans [2]), cela arrive 5 fois (y valant 8 ou 72). Les plus petites sont $a = 791$ et $a = 14330$. On trouve les belles égalités $101249^2 - 791 \cdot 60^4 = 1$ et $1847041^2 - 14430 \cdot 124^4 = 1$. J'ignore s'il y a une infinité de valeurs de a telles que $q^4 - a(2r^2)^2 = 1$ ait une solution.

Passons au cas où x_1 est pair. Alors $a \equiv -1$ modulo 4, de sorte que b et b' sont impairs. Les relations (a') montrent que s et t sont impairs, d'où $b - b' \equiv 2$ modulo 16 et $b + b' \equiv 2q^2$ modulo 16. Si q était impair, $2q^2$ serait congru à 2 ou à 18, soit 2, modulo 16 ; d'où $b + b' \equiv 2$ modulo 16, $2b \equiv 4$ modulo 16 ; en combinant avec $b - b' \equiv 2$ modulo 16, on voit qu'on a $b \equiv 1$ modulo 8 et $b' \equiv -1$ modulo 8.

De plus, si p' est un diviseur premier de b', on a $2q^2 \equiv 1$ modulo p' de sorte que 2 est un carré modulo p', ce qui veut dire $p'^2 \equiv 1$ modulo 16 d'où $p' \equiv \pm 1$ modulo 8 ; comme on a vu que $b' \equiv -1$ modulo 8, cela implique que b' a un nombre impair de facteurs premiers $p' \equiv -1$ modulo 8. De même, pour tout diviseur premier p de b, on a $2q^2 \equiv -1$ modulo p, ce qui veut dire qu'on a soit $p \equiv 1$ modulo 8, soit $p \equiv 3$ modulo 8 ; comme $b \equiv 1$ modulo 8, cela implique que b a un nombre pair de facteurs premiers

$p \equiv 3$ modulo 8. En tous cas, si a a un facteur premier $p \equiv 5$ modulo 8 ($p = 5,\ 13,\ 29,\ 37, \dots$), l'équation ne peut avoir de solution (donc, ici, 1785 n'est pas dans la course).

Tout cela est fort restrictif. Cependant, si l'on considère l'équation $4q^4 - ar^4 = 1$, soit $(2q^2+1)(2q^2-1) = ar^4$, on peut, pour chaque valeur de q, prendre pour a la partie sans facteur carré de $4q^4 - 1$ et voir si le carré restant est un bicarré. Or $2q^2+1$ et $2q^2-1$ sont impairs et premiers entre eux. Comme les nombres impairs sans facteur carré sont nettement plus fréquents que les autres, $2q^2+1$ et $2q^2-1$ seront sans facteur carré, d'où $r = 1$, un bicarré ! Dans ce cas, on prend $a = 4q^4 - 1,\ r = 1$, d'où avec les notations de la démonstration, $x' = 2q^2,\ y' = 1$ pour l'équation initiale, $x = 8q^4 - 1,\ z^2 = 4q^2,\ z = 2q$; pour ces valeurs de q, on a ainsi $(8q^4-1)^2 - (4q^4-1)(2q)^4 = 1$ (facile à vérifier directement). Par exemple, pour $q = 3,\ ar^2 = 17 \cdot 19 = 323$, on trouve $647^2 - 323 \cdot 6^4 = 1$. Pour $q = 4,\ ar^4 = 31 \cdot 33 = 1023$ d'où $2047^2 - 1023 \cdot 8^4 = 1$. Situation analogue pour $q = 6,\ q = 8,\ q = 9$.

D'autres bicarrés que 1 sont possibles. Ainsi, pour $q = 11$, on trouve $2q^2 - 1 = 241$, premier, et $2q^2 + 1 = 243 = 3 \cdot 3^4$; on a alors $a = 3 \cdot 241 = 723,\ r = 3$ et l'égalité $242^2 - 723 \cdot 3^4 = 1$. Pour la valeur “complémentaire” $q = 81 - 11 = 70$ on trouve $2q^2 + 1 = 81 \cdot 121 = 99^2$ et le carré n'est pas un bicarré (l'autre facteur, $2q^2 - 1 = 41 \cdot 239$ est sans facteur carré). On peut continuer et prendre q dans les progressions arithmétiques $81k + 11$, $81k + 70$ de sorte que $3^4 = 81$ divise $2q^2 + 1$; pour les valeurs suivantes, $q = 151$ et $q = 173$, 81 est le facteur carré de $4q^4 - 1$, d'où des solutions avec $a = 2079542403$ et $a = 3582980163$. On peut penser que ce sera le cas général.

De même avec le bicarré $7^4 = 2401$. Ici c'est $2q^2 - 1$ qui est susceptible d'être multiple de 2401. Cela se produit pour $q = 1318$ (alors $2q^2 - 1 = 2401 \cdot 1447$ où 1447 est premier, et $2q^2 + 1 = 3474249$ sans facteur carré), pour son “complémentaire” $2401 - 1318 = 1083$ et probablement pour la plupart des valeurs de q dans les progressions arithmétiques $2401k + 1318$ et $2401k + 1083$.

Dans un autre ordre d'idées, le Théorème 2.2 sur $4x^4 - ay^2 = 1$ montre que, si a est premier, $4q^4 - ar^4 = 1$ ne peut avoir de solution que si $a = 3$ ou $a = 7$; c'est vrai pour $a = 3$, faux pour $a = 7$. On le sait déjà.

Théorème 5.4. *On suppose que U admet un satellite V de norme -1, 2 ou -2. On obtient des solutions de $x^2 - az^4 = 1$ (a sans facteur carré) de la manière suivante :*

1) *Si a est impair $\equiv 1$ modulo 4 et si $N(V) = -1$, il faut et il suffit qu'il existe des entiers q et r tels que $x = 8r^4 + 1,\ z = 2qr$ et $ar^4 = 4q^4 + 1 = (2q^2 + 2q + 1)(2q^2 - 2q + 1)$. Il en existe, déterminant a, si $r = 1$ ou si r est un nombre premier $\equiv 1$ modulo 4. Sauf si $a = 5$, a n'est jamais premier.*

2) *Si a est impair $\equiv -1$ modulo 4 et si $N(V) = 2$ (resp. -2), il faut et il suffit qu'il existe des entiers q et r tels que $x = q^4 - 1$ (resp. $q^4 + 1$), $z = qr$ et $ar^4 = q^4 - 2$ (resp. $q^4 + 2$). Il en existe, pour des valeurs convenables de a, si $r = 1$ ou si r est un nombre premier $\equiv -1$ modulo 8, ou si r est un nombre premier $\equiv 1$ modulo 8 tel que 2 soit un bicarré modulo r (resp. si $r = 1$, si r est premier $\equiv 3$ modulo 8 ou si r est un nombre premier $\equiv 1$ modulo 8 tel que 2 soit un bicarré modulo r).*

3) *Si a est pair, $a = 2a'$ et si $N(V) = 2$ (resp. -2) il faut et il suffit qu'il existe des entiers q et r tels que $x = 16q^4 - 1$, $z = 2qr$ et $a'r^4 = 8q^4 - 1$ (resp. $x = 16q^4 + 1$, $z = 2qr$ et $a'r^4 = 8q^4 + 1$). Il en existe, pour des valeurs convenables de a, si $r = 1$, si r est premier $\equiv -1$ modulo 8 ou si r est un nombre premier $\equiv 1$ modulo 8 tel que 2 soit un bicarré modulo r (resp. si $r = 1$, si r est premier $\equiv 3$ modulo 8 ou si r est un nombre premier $\equiv 1$ modulo 8 tel que 2 soit un bicarré modulo r).*

4) *Dans le dernier cas, a pair, $N(V) = -1$, l'équation n'a pas de solution.*

On élimine les (rares) valeur de a ou a' ayant un facteur carré. L'entier a peut être premier dans le cas 2) ($a = 3, 79, 83, \cdots$) et a' dans le cas 3) ($a' = 7, 127, 647, \ldots$).

Avec les notations du §4, supposons d'abord x_1 impair, ce qui couvre les cas 1), 2), et 4). Soit $u + v\sqrt{a}$ le satellite (de norme positive b) tel que $(u + v\sqrt{a})^2 = b(x + z^2\sqrt{a})$. On a alors, en posant $u = bw$ (cf. §4) :

$$x = 2bw^2 - 1 = 2b'v^2 + 1,\ z^2 = 2vw,\ bw^2 - b'v^2 = 1. \tag{a}$$

Dans le cas 1), on a $b' = 1$, $b = a$ et on a vu que v est pair et w impair. Donc $z^2 = 2vw$ montre que w est un carré r^2 et v de la forme $2q^2$. D'où $ar^4 = 4q^4 + 1 = (2q^2 + 2q + 1)(2q^2 - 2q + 1)$, les deux facteurs étant premiers entre eux. Cette relation est possible si $r = 1$ en prenant $a = 4q^4 + 1$ (s'il est sans facteur carré, ce qui est en général le cas). D'autres valeurs de r sont possibles que, pour alléger, nous supposerons premières. Il s'agit de trouver q tel que $4q^4 \equiv -1$ modulo r^4, ce qui équivaut à $(2q)^4 = 16q^4 \equiv -4$ modulo r^4. Or pour que -4 soit bicarré modulo r^4, il suffit qu'il en soit ainsi modulo r (relèvement classique d'une solution modulo r en une solution r-adique). Pour cela, il faut d'abord que -4 soit un carré modulo r, donc -1 aussi, ce qui veut dire que $r \equiv 1$ modulo 4 ; posons $-1 \equiv i^2$ modulo r. Si 2 est un carré modulo r, on a $r \equiv 1$ modulo 8, l'ordre de F_r^* est multiple de 8, -1 est un bicarré et 2 est un carré ; alors $4 = 2^2$ est un bicarré et -4 également. Si $r \equiv 5$ modulo 8, cet ordre est juste multiple de 4, de sorte que i, et 2 aussi, sont des non-carrés ; ainsi $2i$ est un carré et $-4 = (2i)^2$ est encore un bicarré. Comme $x^4 = 1$ a 4 solutions dans le groupe cyclique $(\mathbf{Z}/\mathbf{Z}r^4)^*$, on obtient 4 progressions arithmétiques de raison r^4 fournissant des valeurs de q telles que $(4q^4 + 1)/r^4$ soit un entier a.

Enfin la formule $ar^4 = (2q^2+2q+1)(2q^2-2q+1)$ montre que, si a est premier, il divise l'un des deux facteurs, l'autre étant un bicarré. Or $2q^2 \pm 2q + 1 = s^4$ donne $2s^4 = (2q \pm 1)^2 + 1$, soit $(2q\pm 1)^2 - 2s^4 = -1$. Par le Lemme 1.4, on a soit $2q \pm 1 = 1$ et $s = 1$ (alors $q = 1$, $ar^4 = 5\cdot 1$, $a = 5$), soit $2q \pm 1 = 239$ et $s = 13$ donnant $q = 119$ ou 120. Pour $q = 119$, $2q^2+2q+1$ ($= 28561$) est bien le bicarré de 13 mais $2q^2 - 2q + 1 = 28085 = 5 \cdot 5617$ est non premier (et sans facteur bicarré). Pour $q = 120$, c'est $2q^2 - 2q + 1$ qui est le bicarré de 13, et $2q^2 + 2q + 1 = 29401 = 113 \cdot 257$ n'est pas premier.

Exemples. – Si $r = 1$, les valeurs successives de $a = 4q^4 + 1$ sont 5, 65, 325 (éliminé car facteur carré), 1025 (éliminé), $2501 = 41 \cdot 61$, $5185 = 61 \cdot 5 \cdot 17$, $9605 = 5 \cdot 17 \cdot 113$. Pour $q \equiv 2$ ou 3 modulo 25, on élimine à cause du facteur carré 25.

– Si $r = 5$, $r^4 = 625$, les 4 progressions arithmétiques de raison 625 fournissant de "bonnes" valeurs de q ont pour premiers termes 221, 222 et leurs complémentaires 403, 404. Les valeurs correspondantes de a, $157 \cdot 97241$, $157 \cdot 99013$, $521 \cdot 324013$ et $521 \cdot 327241$ sont sans facteur carré.

Dans le cas 3) avec $a = 2a'$ et $N(V) = 2$, on a $b = 2$, $b' = a'$, $2w^2 - a'v^2 = 1$ (voir (a)), de sorte que $a'v^2$ et v sont impairs. Ainsi $z^2 = 2vw$ montre que v est un carré r^2 et w de la forme $2q^2$. Les formules (a) montrent alors qu'on a $x = 16q^4 - 1$, $z = 2qr$ et $a'r^4 = 8q^4 - 1$. C'est possible pour $r = 1$ en prenant $a' = 8q^4 - 1$. Pour r premier, on doit avoir $8q^4 \equiv 1$ modulo r^4, soit $(2q)^4 \equiv 2$ modulo r^4. Comme ci-dessus, il suffit pour cela que 2 soit un bicarré modulo r. En particulier 2 est un carré modulo r, ce qui veut dire $r \equiv \pm 1$ modulo 8. Si $r \equiv -1$ modulo 8, $t \mapsto t^4$ a, dans F_r^*, le même noyau $\{1, -1\}$, que $t \mapsto t^2$ ce qui montre que tout carré est un bicarré ; les valeurs possibles de q forment alors deux progressions arithmétiques de raison r^4. Si $r \equiv 1$ modulo 8, ce la dépend de la valeur de r ; si 2 est bien un bicarré, il y a 4 progressions arithmétiques de raison r^4 pour les valeurs de q.

On constate que 2 est un bicarré modulo r (premier $\equiv 1$ modulo 8) pour $r = 73, 89, 113, 161, 217, 233, \dots$ et n'en est pas un pour $r = 17, 41, 97, 137, 193, 241, \dots$. Que 2 soit un carré modulo r veut dire que r est décomposé dans $A = \mathbf{Z} + \mathbf{Z}\sqrt{2}$, soit $r = (s + t\sqrt{2})(s - t\sqrt{2})$ car cet anneau est principal. Il faut alors voir si $s + t\sqrt{2}$ (resp. $s - t\sqrt{2}$) est inerte ou décomposé dans $B = A + A\sqrt[4]{2}$ (qui est d'ailleurs principal aussi).

Lorsque r est de la forme $r = 8s + 1$ avec s impair, il y a un critère simple pour savoir si 2, ou d'ailleurs n'importe quel entier d (premier à r), est un bicarré modulo r. En effet, F_r^* est composé direct d'un sous-groupe cyclique d'ordre s et d'un sous-groupe cyclique G d'ordre 8, la projection sur ce dernier étant $t \mapsto t^s$. Comme les seuls bicarrés dans G sont 1 et -1, le critère est "$d^s \equiv 1$ modulo r".

Exemples. – Pour $r = 1$, les valeurs successives de $a' = 8q^4 - 1$ sont 7, 127, 647, 2047, 4999, ... ; certaines sont premières. Comme le polynôme $8X^4 - 1$ est irréductible (appliquer Eisenstein à son double $(2X)^4 - 2$), une conjecture jugée plausible dit qu'il prend une infinité de valeurs premières (cf. [6]).

– Pour $r = 7$, les 2 progressions arithmétiques de raison $7^4 = 2401$ ont pour premiers termes $q = 1160$ et $q = 1261$

Dans le cas 3) avec $N(V) = -2$, on a $b' = 2$, $b = a'$, $a'w^2 - 2v^2 = 1$, c'est w qui est impair. Comme $z^2 = 2vw$, on peut poser $w = r^2$ et $v = 2q^2$. Les formules (a) donnent alors $x = 16q^4 + 1$, $z = 2qr$ et $a'r^4 = 8q^4 + 1$. C'est possible pour $r = 1$ en prenant $a' = 8q^4 + 1$. Pour r premier, il faut voir ici si -2 peut être un bicarré modulo r^4, c'est-à-dire modulo r. Si $r \equiv -1$ modulo 4, -1 est un non-carré, donc -2 sera un carré ssi 2 est un non-carré, ce qui veut dire $r \equiv 3$ modulo 8 ; comme, dans ce cas, tout carré est un bicarré, cette condition suffit et il y a deux progressions arithmétiques de raison r^4 fournissant les valeurs possibles de q. Si $r \equiv 1$ modulo 4, -1 est un carré, donc 2 doit en être un, ce qui veut dire $r \equiv 1$ modulo 8, mais que 2 soit un bicarré dépend de la valeur de r (voir ci-dessus) ; en ce cas, 4 progressions arithmétiques de raison r^4 pour les valeurs possibles de q.

Exemples. – Pour $r = 1$, les premières valeurs de $a' = 8q^4 + 1$ sont 9 (éliminé, carré), 129 ($= 3 \cdot 43$), 649 ($= 11 \cdot 59$), 2049 ($= 3 \cdot 683$), 5001 ($= 3 \cdot 1667$), 10369 (enfin premier), ...

– Pour $r = 3$, $8q^4 \equiv -1$ modulo 81, les premiers termes des progressions arithmétiques de raison 81 sont 17 et 64 ; pour $q = 17$ on trouve $a' = 8249 = 73 \cdot 113$ pour $q = 64$, on trouve $a' = 1657009$.

Dans le cas 4), on a $b' = 1$, $b = a = 2a'$, les formules (a) donnant $x = 2v^2 + 1$, $z^2 = 2vw$ et $2a'w^2 - v^2 = 1$. Ainsi v est impair et $2a'w^2 = v^2 + 1 \equiv 2$ modulo 4 montre que w est impair aussi, de sorte que $z^2 = 2vw$ est impossible (voir aussi à la fin du §4).

Voyons enfin le cas 2) ($a \equiv -1$ modulo 4, $N(V) = \pm 2$). Pour le satellite $u + v\sqrt{a}$ de norme positive b tel que $(u + v\sqrt{a})^2 = b(x + z^2\sqrt{a})$, on a, comme x_1 est pair, les formules (cf. §4) :

(a') $$x = bw^2 - 1 = b'v^2 + 1,\ z^2 = vw \text{ et } bv^2 - b'w^2 = 2\ (u = bw).$$

En tous cas, v et w sont des carrés. Si $N(V) = 2$ on a $b = 1$, $b' = a$ et on pose $w = q^2, v = r^2$ de sorte que $x = q^4 - 1$, $z = qr$ et $ar^4 = q^4 - 2$. C'est possible si $r = 1$ en prenant $a = q^4 - 2$, q impair. Pour r premier, on est ramené à à voir si 2 est un bicarré modulo r, question déjà traitée dans le cas 3).

Exemples. – Pour $r = 1$, on obtient $a = 79$ (premier), $a = 623 = 7 \cdot 89$, $a = 2399$ premier, et $X^4 - 2$ étant irréductible (Eisenstein), il est plausible qu'on obtienne une infinité de valeurs premières de a.

- Pour $r = 7$, on obtient, pour q, 2 progressions arithmétiques de raison $7^4 = 2401$, dont on élimine les valeurs paires (a devant être impair). Leurs premiers termes sont 121, donnant $a = 89729 = 53 \cdot 1693$, et 2280 (éliminé).

Si $N(V) = -2$ on a $b = a$, $b' = 1$ et on pose $v = q^2$, $w = r^2$. D'où $x = q^4 + 1$, $z = qr$ et $ar^4 = q^4 + 2$. C'est possible pour $r = 1$ en prenant $a = q^4 + 2$ avec q impair. Pour r premier, $q^4 + 2 \equiv 0$ modulo r^4, il faut voir quand -2 est un bicarré modulo r, question traitée dans le cas 3) : prendre $r \equiv 3$ modulo 8, ou $r \equiv 1$ modulo 8 pour certaines valeurs de r.

Exemples. – Pour $r = 1$, q impair, on obtient $a = 3$, $a = 83$ premier, $a = 627 = 3 \cdot 11 \cdot 19$, $a = 2403 = 3^2 \cdot 267$ éliminé pour cause de carré, et, plausiblement une infinité de valeurs premières.

- Pour $r = 3$, on obtient, pour q, 2 progressions arithmétiques de raison $3^4 = 81$ dont on élimine les valeurs paires et dont les premiers termes sont 34 (éliminé) et 47 (donnant $a = 60243 = 3 \cdot 43 \cdot 467$) ; pour $q = 34 + 81 = 115$, on trouve $a = 174900627$.

Je remercie vivement Maurice Mignotte et Paulo Ribenboim de m'avoir fourni informations, conseils et encouragements.

Bibliographie

[1] J. H. E. COHN, *The Diophantine equation* $x^4 - Dy^2 = 1$. Quart. J. Math. Oxford Ser. (2) **26** (1975), no. 103, 279–281.

[2] J. H. E. COHN, *The Diophantine equation* $x^4 - Dy^2 = 1$. *II*. Acta Arith. **78** (1997), 401–403.

[3] W. LJUNGGREN, *Über die Gleichung* $x^4 - Dy^2 = 1$. Arch. Math. Naturv., Olso, **45** (1942), n°5, 61–70.

[4] W. LJUNGGREN, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$. Avh. Norsk. Vid. Akad. Olso, (1942), 1–27.

[5] W. LJUNGGREN, *Ein satz über die diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$. Tolfte Skand. Math. Kongresses, Lund, 1953, pp. 188–194. Lunds Universitets Matematiska Inst., Lund, (1954).

[6] P. RIBENBOIM, *Nombres premiers, mystères et records*. Presses Universitaires de France, Paris, 1994, pp. 217–218.

Pierre SAMUEL
3, avenue du Lycée Lakanal
92340 Bourg la Reine
France