JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Pierre SAMUEL

Les carrés dans des généralisations des suites de Lucas

Tome 16, n° 3 (2004), p. 693-703.

<http://jtnb.cedram.org/item?id=JTNB_2004__16_3_693_0>

Journal de Théorie des Nombres
de Bordeaux **16** (2004), 693–703

Les carrés dans des généralisations des suites de Lucas

par Pierre SAMUEL

Résumé. Etant donnés deux entiers P, Q, impairs, premiers entre eux et tels que $P^2 - 4Q > 0$, on étudie les suites $(x_n)_{n\geqslant 0}$ d'entiers positifs telles que $x_{n+1} = Px_n - Qx_{n-1}$. Elles généralisent les suites classiques de Lucas $(U_n(P,Q))$ et $(V_n(P,Q)$. Les propriétés des diviseurs premiers de $V_n(P,Q)$ pour $n = 3 \cdot 2^j$ donnent, via le calcul des Symboles de Legendre de certains x_n modulo ceux-ci, une méthode efficace de détermination des carrés (resp. doubles, triples, ... de carrés) dans une suite (x_n). Ceci est appliqué aux équations Diophantiennes de la forme $x^4 - Ey^2 = k$, $x^2 - Ey^4 = k$ lorsque E est la partie sans facteurs carrés d'un entier de la forme $P^2 - 4$, P impair. On construit des suites (x_n) contenant un carré d'indice arbitrairement grand. Et on montre comment trouver des suites (x_n) contenant trois carrés.

Abstract. Let P, Q be positive, relatively prime and odd integers such that $P^2 - 4Q > 0$. We study the sequences $(x_n)_{n\geqslant 0}$ of positive integers satisfying the recursion formula $x_{n+1} = Px_n - Qx_{n-1}$. They generalize the classical Lucas sequences $(U_n(P,Q))$ and $(V_n(P,Q))$. The prime divisors of $V_n(P,Q)$ for $n = 3 \cdot 2^j$ have nice properties which, through the computation of the Legendre Symbols of suitable x_n's modulo these primes, give an efficient method for trying to find all squares (also double squares, triple squares, ...) in the sequence (x_n). This is applied to Diophantine equations of the form $x^4 - Ey^2 = k$, $x^2 - Ey^4 = k$ when E is the squarefree part of an integer $P^2 - 4$, P odd. We construct sequences (x_n) containing squares with arbitrarily large indices. We also show how to find sequences (x_n) containing three squares.

1. Introduction

Soient P et Q deux entiers positifs premiers entre eux tels que $D = P^2 - 4Q$ soit positif. On pose $\alpha = \frac{1}{2}(P + \sqrt{D})$, $\beta = \frac{1}{2}(P - \sqrt{D})$. Ce sont

Manuscrit reçu le 29 octobre 2003.

des entiers algébriques car ils ont P pour trace et Q pour norme. Ainsi $2\alpha^n$ a des coefficients entiers et on pose

$$2\alpha^n = V_n + U_n\sqrt{D}. \quad \text{(voir note (1))}$$

On pose également $U_{-n} = -1/Q^n U_n$ et $V_{-n} = 1/Q^n V_n$. Les suites (V_n) (ou $V_n(P,Q)$) et (U_n) (ou $(U_n(P,Q))$ sont les classiques suites de Lucas. Rappelons les formules (cf. [3])

$$V_0 = 2,\ V_1 = P,\ V_2 = P^2 - 2Q; \quad U_0 = 0,\ U_1 = 1,\ U_2 = P;$$

$$V_{n+1} = PV_n - QV_{n-1},\ U_{n+1} = PU_n - QU_{n-1}; \quad V_n^2 - DU_n^2 = 4Q^n.$$

P. Ribenboim et W.Mc Daniel ([3]) ont brillament déterminé tous les carrés (et doubles de carrés) dans les suites $(V_n(P,Q))$ et $U_n(P,Q))$ lorsque P et Q sont impairs. En supposant encore P et Q impairs, nous étudions ici les carrés dans les suites (x_n) plus générales qui satisfont seulement la relation de récurrence

$$x_{n+1} = Px_n - Qx_{n-1}. \tag{1}$$

Pour P et Q fixés, une telle suite est déterminée par les entiers x_0 et x_1. Alors chaque x_n, $n \geqslant 0$ est un entier (tandis que x_{-j} est un nombre rationnel dont Q^j est un dénominateur). Assurons nous que les x_n sont tous positifs.

Ceci signifie :

$$x_1/x_0 \geqslant \beta = \frac{1}{2}(P - \sqrt{D}). \tag{2}$$

Démonstration. Posons $t_n = x_{n+1}/x_n$. on a $t_n = P - (Q/t_{n-1})$. On examine le graphe (concave) de $f(t) = P - (Q/t)$ et l'itération de f. On voit :
- Si t_0 est plus grand que la grande racine α de $f(t) = t$, la suite (t_n) décroit et tend vers α. C'est le cas si $x_n = U_n$.
- Si t_0 est entre les racines β et α de $f(t) = t$, la suite (t_n) croit et tend encore vers α. C'est le cas si $x_n = V_n$.
- Si $t_0 < \beta$, la suite (t_n) devient négative et tend vers $-\infty$.

On voit de même que les nombres $x_{-j} (j \geqslant 0)$ sont négatifs si $x_1 > \alpha x_0$ et positifs si $\beta x_0 < x_1 < \alpha x_0$. □

2. Quelques résultats utiles

Soit (x_n) une suite de Lucas généralisée telle que $x_{n+1} = Px_n - Qx_{n-1}$. Soient y_0 et y_1 les entiers tels que $y_1 + x_1\sqrt{D} = \alpha(y_0 + x_0\sqrt{D})$ (c'est à dire $y_0 = 2x_1 - Px_0,\ y_1 = Px_1 - 2Qx_0$). Posons $y_n + x'_n\sqrt{D} = \alpha^n(y_0 + x_0\sqrt{D})$. On a $y_{n+k} + x'_{n+k}\sqrt{D} = \alpha^k(y_n + x'_n\sqrt{D}) = \frac{1}{2}(V_k + U_k\sqrt{D})(y_n + x'_n\sqrt{D})$, d'où $2x'_{n+k} = V_k x'_n + U_k y_n$.

De même, si $n - k \geqslant 0$, on a $y_{n-k} + x'_{n-k}\sqrt{D} = \alpha^{-k}(y_n + x'_n\sqrt{D}) = \frac{1}{2}Q^{-k}(V_k - U_k\sqrt{D})(y_n + x'_n\sqrt{D})$, d'où $2Q^k x'_{n-k} = V_k x'_n - U_k y_n$.

Par addition, on obtient $x'_{n+k} + Q^k x_{n-k} = V_k x'_n$. Pour $k = 1$, ceci donne $x'_{n+1} = Px'_n - Qx'_{n-1}$. Donc, comme $x'_0 = x_0$ et $x'_1 = x_1$ et comme les suites (x'_n), (x_n) satisfont la même relation de récurrence, on a $x'_n = x_n$ pour tout n. D'où

$$x_{n+k} + Q^k x_{n-k} = V_k x_n \tag{3}$$

ce qui équivaut à $x_{n+2k} + Q^k x_n = V_k x_{n+k}$.

On déduit aussitôt de (3) des propriétés des Symboles de Legendre :

Théorème 1. *Soient $(x_n)_{n\geqslant 0}$ une suite d'entiers positifs telle que $x_{n+1} = Px_n - Qx_{n-1}$, et p un diviseur premier impair de V_k. Alors :*
a) Si k est pair, on a $(\frac{x_{n+2k}}{p}) = (\frac{-1}{p})(\frac{x_n}{p})$, de sorte que $(\frac{x_{n+2k}}{p})$ et $(\frac{x_n}{p})$ sont égaux si $p \equiv 1 \mod 4$ et opposés si $p \equiv -1 \mod 4$.
b) Si k est impair, on a $(\frac{x_{n+2k}}{p}) = (\frac{-1}{p})(\frac{Q}{p})(\frac{x_n}{p})$.

Nous écrirons parfois $V(k)$ au lieu de v_k . Pour appliquer efficacement le Th.1, nous avons besoin d'informations sur les diviseurs premiers de $V(k)$. C'est le cas lorsque $k = 3 \cdot 2^j$ $(j \geqslant 1)$. Rappelons les formules ([3]) :

$$V_{3n} = V_n(V_n^2 - 3Q^n), \quad V_{2n} = V_n^2 - 2Q^n.$$

On suppose désormais P et Q impairs. Pour $n = 2^j$, la seconde formule montre par récurrence sur j que $V(2^j)$ est impair et, de plus, pour $j \geqslant 1$, que $V(2^j) \equiv 1 \pm 2 \mod 4$, soit $V(2^j) \equiv -1 \mod 4$ et ce nombre admet un diviseur premier $p \equiv -1 \mod 4$. L'autre facteur, $V(2^j)^2 - 3Q^{2^j}$ de $V(3 \cdot 2^j)$ est congru à $1 - 3 \equiv 6$ modulo 8 et s'écrit donc sous la forme $2W$ avec $W \equiv -1 \mod 4$; il admet donc aussi un diviseur premier $p' \equiv -1 \mod 4$.

Peut-on avoir $p = p'$? Dans ce cas p divise $V(2^j)$ et $3Q^{2^j}$. Or, comme P est premier à Q et que $V_{n+1} \equiv PV_n \mod Q$, tous les V_n sont premiers à Q et donc p aussi. On doit donc avoir $p = p' = 3$ et Q est premier à 3. Mais pour n pair, la formule $V_{2n} = V_n^2 - 2Q^n$ lue modulo 3 montre que V_{2n} est premier à 3, ce qui contredit $p = 3$ lorsque $2n = 2^j$ avec $j \geqslant 2$. On a ainsi démontré :

Théorème 2. *On suppose P et Q impairs. Alors $V(3\cdot 2^j)$ admet un diviseur premier $p \equiv -1 \mod 4$ et au moins deux pour $j \geqslant 2$.*

Le cas spécial pour $j = 1$ peut se produire. Pour $(P, Q) = (7, 5)$ on a $V_6 = (3 \cdot 13)(2 \cdot 3 \cdot 41)$ et 3 est le seul diviseur premier $\equiv -1 \mod 4$ de V_6. Cela ne se produit que si $Q \equiv -1 \mod 3$.

Théorème 3. *On suppose P et Q impairs. Si un x_a est un carré et est, pour tout j, premier à un diviseur premier $p_j \equiv -1 \mod 4$ de $V(3 \cdot 2^j)$, alors aucun x_{a+12q}, $q \neq 0$ n'est un carré.*

Démonstration. Posons $q = 2^{j-1}q'$ avec q' impair et $j \geqslant 1$. La formule du binôme appliquée à $(V(3\cdot 2^j) + U(3\cdot 2^j)\sqrt{D})^{q'}$ montre que $V(6q)$ est un multiple de $V(3\cdot 2^j)$. En appliquant le Théorème 1, a) avec $n = a$ et $k = 6q$, on voit que x_{a+12q} est un non-carré modulo p_j et ne peut donc être un carré. □

Compléments : Montrons qu'un diviseur premier impair p de x_a divise au plus un des $V(3\cdot 2^j)$. En effet, de $V_{2n} \equiv -2Q^n \mod V_n$ on déduit $V_{4n} - 2Q^{2n} \equiv 4Q^{2n} - 2Q^{2n} = 2Q^{2n} \mod V_n$ et $V(2^h n) \equiv 2Q^{2^{h-1}n} \mod V_n$ pour tout $h \geqslant 2$. Donc, comme Q est premier à tous les V_s, $V(2^h n)$ est premier à V_n pour tout h. Il n'y a donc qu'un nombre fini d'exposants j pour lesquels la condition du Th.3 n'est pas satisfaite.

Soit r le radical de x_a. On peut parfois montrer que r est premier à tous les $V(3\cdot 2^j)$ (ou même à tous les V_n). Si $r = 2$, il est évidemment premier à tous les p_j de l'énoncé.

Si r est premier et s'il y a plusieurs diviseurs premiers $p_j \equiv -1 \mod 4$ de $V(3\cdot 2^j)$ (vrai pour $j \geqslant 2$ par le Th.2), r est premier à l'un deux et la condition du Th.3 est satisfaite.

Pour r premier, le seul "mauvais cas" est $r = 3$, $j = 1$, 3 étant le seul diviseur premier $\equiv -1 \mod 4$ de V_6. Exemple : pour $P = 7$, $Q = 11$, $V_6 = 2\cdot 81\cdot 61$ on prend $x_0 = 81$, $x_1 = 146735$ et on obtient $x_{12} = 2482587^2$.

Remarque : Supposons que, pour tout j, il y ait un diviseur premier impair p_j de $V(3\cdot 2^j)$ qui soit premier au carré x_a et qu'on ait, soit $p_j \equiv -1 \mod 4$ et $(\frac{Q}{p_j}) = 1$, soit $p_j \equiv 1 \mod 4$ et $(\frac{Q}{p_j}) = -1$. Alors, par le Th.1, b), aucun x_{a+6q}, $q \neq 0$ n'est un carré..

Premières conclusions.

Une suite de Lucas généralisée ne contient qu'un nombre fini de carrés. En effet, par le Th.3 et ses compléments, il en est ainsi pour chaque classe d'indices modulo 12. J'ai rencontré des suites contenant 4 carrés. Voir aussi § 6.

Il en est de même pour les multiples donnés de carrés (doubles, triples ... de carrés). En effet, si x_n est, disons, le triple d'un carré, alors $3x_n$ est un carré, et inversement car alors $3x_n$ est un multiple de 9 ; on est ainsi ramené aux carrés dans la suite $(3x_n)$.

La "square class" d'un élément x_b d'une telle suite (c'est à dire les x_j tels que x_b et x_j aient la même partie sans facteurs carrés) est finie : on est ramené aux carrés dans la suite $(x_b x_j)_j$.

3. Une méthode de recherche des carrés

Nous supposons P et Q impairs et premiers entre eux et nous cherchons à trouver tous les carrés dans une suite (x_n) telle que $x_{n+1} = Px_n - Qx_{n-1}$.

On commence par chercher des entiers b simples tels que 12 soit une période de la suite (x_n) modulo b (ou de $(\frac{x_n}{b})$ si b est premier). C'est toujours le cas si $b = 8$ ou est un diviseur premier P ou Q. C'est parfois le cas pour $b = 3, 9, 5$ (voir note (2)). Soit alors I l'ensemble des indices a, $0 < a \leqslant 12$, tels que x_a soit un carré modulo tous ces entiers b. Ainsi, si x_n est un carré, il y a un $a \in I$ tel que $n \equiv a \mod 12$.

Il arrive que I soit vide, et la recherche est alors terminée.

Cela fait, et si x_a est un carré, le Th.3 et ses compléments permettent souvent de conclure que la sous-suite (x_{a+12n}) n'en contient pas d'autre. Sinon, un nombre fini d'indices j est impliqué et l'on voit si les valeurs correspondantes de x_{a+12n} sont des carrés.

Pour les autres sous-suites (x_{a+12n}) $(a \in I)$ on commence par tester x_a modulo les diviseurs premiers de V_6 :

A) Si un diviseur premier $q \equiv 1 \mod 4$ de V_6 est disponible et si x_a est un non-carré modulo q, alors aucun x_{a+12n} n'est un carré (Th.1).

Sinon :

B) Soit $p \equiv -1 \mod 4$ un diviseur premier de V_6. Si $(\frac{x_a}{p}) = 1$ (resp. -1), alors les termes $x_{a+12+24n}$ (resp. x_{a+24n}) ne peuvent être des carrés. D'où trois cas :

B.1) Il y a deux diviseurs premiers $p, p' \equiv -1 \mod 4$, de V_6 tels que $(\frac{x_a}{p})$ et $(\frac{x_a}{p'})$ sont opposés. Alors aucun x_{a+12n} n'est un carré.

B.2) x_a est un carré modulo tous les diviseurs premiers $p \equiv -1 \mod 4$ de V_6. Alors il reste à étudier les x_{a+24n} et l'on teste x_a encore, cette fois modulo les diviseurs premiers de V_{12}.

B.3) x_a est un non-carré modulo tous les diviseurs premiers $p \equiv -1 \mod 4$ de V_6. Restent alors à étudier les $V_{a+12+24n}$ et on teste x_{a+12} (ou x_{a-12}) modulo les diviseurs premiers de V_{12}. (voir note (3))

Et ainsi de suite : on effectue des tests modulo les diviseurs premiers de $V_6, V_{12}, V_{24}, \ldots$ jusqu'à ce qu'on se trouve dans une "bonne" situation A) ou B.1) (ou jusqu'à ce qu'un carré inattendu soit découvert). Cette méthode est fort efficace : j'ai étudié 1661 suites et seules 37 ont résisté aux tests V_6 et V_{12}. (voir notes (4) et (5))

Exemple 1. Suites $x_{n+1} = 5x_n - 3x_{n-1}$. On a $D = 13$, $V_6 = 2 \cdot 19 \cdot 167$ et $V_{12} = 2 \cdot 7^3 \cdot 47 \cdot 1249$ (facteurs premiers).

Pour la suite commençant par $1, 5$, les congruences modulo $8, 3, 5$ demandent $a \equiv 0$ ou $4 \mod 12$. Le cas $a = 0$ est réglé par le Th.3 ($x_0 = 1$). On a $x_4 = 409, (\frac{409}{19}) = -1, (\frac{409}{167}) = 1$, "bon" cas B.1). Donc x_0 est le seul carré.

Pour la suite commençant par $1, 13$, les congruences demandent $a = 0, 7, 11$. Le Th.3 règle le cas $a = 0$. On a $x_7 = 93169, (\frac{93169}{19}) = -1, (\frac{93169}{167}) = 1$, "bon" cas B.1). Mais $x_{11} = 3723516$ est un carré modulo 19 et 167 ; donc

on le passe au test V_{12} et on voit que c'est un non carré modulo 1249, bon cas A). Donc x_0 est le seul carré dans cette suite.

Exemple 2. Suites $x_{n+1} = 7x_n - 3x_{n-1}$. On a $D = 37$, $V_6 = 2 \cdot 43 \cdot 911$ et $V_{12} = 2 \cdot 431 \cdot 1831 \cdot 3889$.

Pour la suite qui commence par $1, 4$, les congruences modulo $3, 7, 8, 5$ demandent $a = 0, 1, 2, 8, 11$. Les cas $a = 0, 1$ sont règlés par le Th.3. Le cas $a = 2$ également car $x_2 = 25 = 5^2$ et car 5 est premier à tous les V_n. Le terme x_8 est un carré modulo 43 et 911, cas B.2), mais un non-carré modulo le facteur 3889 deV_{12}, bon cas A). Enfin, au lieu de x_{11}, on calcule x_{-1} et on trouve $x_{-1} = 1$. La suite contient donc juste 4 carrés 1,1,4,25.

Avec la suite commençant par $1, 3$, les congruences demandent $a = 0, 4, 6, 10$. Pour $a = 0$, on applique le Th.3. Le terme $x_6 = 9 \cdot 3637$ est un carré modulo 43 et 911, cas B.2), mais un non carré modulo 3889, cas A). Mais x_4 et x_{10} sont des non-carrés modulo 43 et 911, cas B.3) ; on doit donc passer x_{16} et x_{22} (ou x_{-8} et x_{-2}) au test V_{12} : tous deux sont des non-carrés modulo 3889, cas A). Ainsi $x_0 = 1$ est le seul carré de la suite.

4. Application à certaines équations diophantiennes

Nous prenons ici $Q = 1$ et, comme toujours, P impair. De 3 en 3, une suite (x_n) telle que $x_{n+1} = Px_n - x_{n-1}$ satisfait à $x_{n+3} + x_{n-3} = V_3 x_n = P(P^2 - 3)x_n$ et $P(P^2 - 3)$ est un nombre pair $2s$ où s est impair. Or on rencontre des suites (v_j), (u_j) satisfaisant des relations de récurrence de la forme $v_{j+1} = 2sv_j - v_{j-1}$, idem u_j, dans la recherche des solutions d'équations de la forme

$$u^2 - Ev^2 = k \quad \text{(E sans facteurs carrés).} \tag{4}$$

En effet on sait que celles-ci, (u_j, v_j) forment un nombre fini de familles $u_j + v_j\sqrt{E} = (u_0 + v_0\sqrt{E})(s + t\sqrt{E})^j$, où $\gamma = s + t\sqrt{E}$ est la plus petite unité de norme 1 contenue dans $\mathbb{Z} + \mathbb{Z}\sqrt{E}$. Les relations de récurrence sont satisfaites par les suites (u_j) et(v_j). Ainsi la recherche des solutions des équations biquadratiques

$$x^4 - Ey^2 = k\ , \quad x^2 - Ey^4 = k \tag{5}$$

se ramène à celle des carrés dans les suites (u_j), (v_j).

Pour insérer une telle suite, disons (v_j) (avec $Q = 1$), il faut et il suffit qu'on ait

$$2s = P(P^2 - 3)\ , \text{ c'est à dire } \gamma = \alpha^3. \tag{6}$$

Ceci veut dire que Q contient une unité de norme 1 de la forme $\frac{1}{2}(a + b\sqrt{E})$ $(= \alpha)$ avec a et b impairs, ou encore que $x^2 - Ey^2 = 4$ a une solution impaire. Alors $a = P$, E est la partie sans facteurs carrés de $D = P^2 - 4$, $D = ER^2$ et alors $b = R$.

La condition que $x^2 - Ey^2 = 4$ a des solutions impaires a parfois été utilisée par J.H.E. Cohn ([1],[2]) (qui utilisait plus souvent la condition plus forte que $x^2 - Ey^2 = -4$ a des solutions impaires).

Les discriminants E qui satisfont notre condition sont tous $\equiv 5 \mod 8$. Les premiers sont $E = 5$, 13, 21, 29. Parmi les 53 entiers $E \leqslant 500$, $E \equiv 5 \mod 8$, sans facteurs carrés, seuls 9 ne satisfont pas cette condition (ce sont 37, 101, 127, 269, 349, 373, 381, 389 et 485).

Supposons cette condition satisfaite. L'insertion d'une suite (v_j) dans une suite de Lucas généralisée (x_n) demande qu'on ait $x_0 = v_0$, $x_3 = v_1$. Comme $x_3 = (P^2 - 1)x_1 - Px_0$, soit $(P^2 - 1)x_1 = v_1 + Pv_0$, x_1 n'est pas nécessairement un entier, mais on peut le rendre entier en multipliant par un carré convenable (ce qui ne modifie pas les résultats des tests sur les termes déjà entiers) ; d'où une suite (x'_n). Ainsi la solutions des équations (5) se ramène à détermination des carrés (d'indices multiples de 3) dans de telles suites (x'_n).

Avec des moyens de calcul assez rudimentaires (et en allant rarement plus loin que les tests V_6 et V_{12}), j'ai étudié 5272 équations (5) (pour les discriminants 5, 13, 21, 29, 53 et 77) et n'ai pû conclure que dans 38 cas (voir note (5)).

Exemple 1. Prenons $P = 3$ et donc $D = E = P^2 - 4 = 5$. On a $2s = 18$. L'équation $u^2 - 5v^2 = 11$ a deux familles de solutions :

$$u_j + v_j\sqrt{5} = (4 + \sqrt{5})(9 + 4\sqrt{5})^j \text{ et } u_j + v_j\sqrt{5} = (16 + 7\sqrt{5})(9 + 4\sqrt{5})^j$$

La première suite (u_j) commence par 4, 56, la seconde par 16, 284. Elles "connectent" : en posant $u_0 = 4$, on a $u_{-1} = 16$. Si l'on cherche une suite (x_n) telle que $x_0 = 4$ et $x_3 = 56$, on trouve $8x_1 = 68$, $x_1 = 8,5$ et on doit multiplier par 4. D'où la suite $x'_n = 16$, 34, 86, 224. Modulo 3, on doit avoir $n \equiv 0$, $1 \mod 4$ et modulo 8, $n \equiv 0 \mod 3$. Restent les indices $n \equiv 0$, $9 \mod 12$. Or $x_{-3} = 64$ un carré. Le Th.3 montrent que ce sont les seuls. Donc les seules solutions de $x^4 - 5y^2 = 11$ sont $(2, 1)$ et $(4, 7)$.

La seconde suite (v_j) : 7, 127, 2279 a tous ses termes $\equiv 3 \mod 4$ et ne contient donc aucun carré. La première commence par 1, 25, 449. Si l'on cherche une suite (x_n) telle que $x_0 = 1$, $x_3 = 25$, on trouve $8x_1 = 28$, $x_1 = 3,5$ et on doit multiplier par 4. D'où la suite (x'_n) : 4, 14, 38, 100. Modulo 3, on doit avoir $n \equiv 0$, $3 \mod 4$ et, modulo 4, $n \equiv 0 \mod 3$. Restent $n \equiv 0$, 3, des carrés. Par le Th.3, on voit que les seules solutions de $x^2 - 5y^4 = 11$ sont $(4, 1)$ et $(56, 5)$.

Exemple 2. On prend $P = 5$, d'où $D = E = 21$. L'unité fondamentale γ est $55 + 12\sqrt{21}$, d'où $2s = 110$. Il y a deux familles de solutions de $u^2 - 21v^2 = -5$ dont les termes initiaux $u_0 + v_0\sqrt{21}$ sont $4 + \sqrt{21}$ et $32 + 7\sqrt{21}$.

La première suite (u_j) commence par 4, 472. Dans une suite (x_n) telle que $x_0 = 4$ et $x_3 = 472$, on doit avoir $24x_1 = 492$, $2x_1 = 41$ et l'on doit multiplier par 4. D'où la suite (x'_n) : 16, 82, 394, 1888... Les indices impairs sont éliminés modulo 5 et on doit avoir, modulo 8, $n \equiv 0,\ 6 \mod 12$. Mais, en opérant modulo 11 (voir note (2)), on voit que $n \equiv 6$ est éliminé. Reste $n = 0$, un carré, et on applique le Th.3.

L'autre suite (u_j) commence par 32, 3524... Dans une suite (x_n) telle que $x_0 = 32$, $x_3 = 3524$, on doit avoir $24x_1 = 3684$, d'où $x_1 = 153,5$ et l'on doit multiplier par 4. D'où la suite (x'_n) : 128, 614, 2942, 14096 ... Modulo 8, on doit avoir $n \equiv 0,\ 3,\ 6,\ 9 \mod 12$. Les indices pairs sont éliminés modulo 5. Comme x'_3 est un carré modulo 11, $n \equiv 9$ est éliminé (cf. note (2)). Reste à passer x'_3 au test $V_6 = 2 \cdot 23 \cdot 263$. Or 14096 est un non-carré modulo 23 et un carré modulo 263, "bon" cas B.1), qui l'élimine. Cette suite (uj) ne contient donc pas de carrés et la seule solution de $x^4 - 21y^2 = -5$ est $(2, 1)$.

Les suites (v_j), qui commencent par 1, 103 et par 7, 769, "connectent" : si l'on pose $u_0 = 1$, $u_1 = 103$, on a $u_{-1} = 7$, $u_{-2} = 769$. Dans une suite (x_n) telle que $x_0 = 1$ et $x_3 = 103$, on doit avoir $24x_1 = 108$, d'où $x_1 = 4,5$ et on multiplie par 4. D'où la suite (x'_n) : 4, 18, 86, 412 ... Modulo 8, on doit avoir $n \equiv 0,\ 3,\ 6,\ 9 \mod 12$. Les indices impairs sont éliminés modulo 5 et $n \equiv 6$ modulo 11. Reste $x'_0 = 4$, seul carré par le Th.3. La seule solution de $x^2 - 21y^4 = -5$ est donc $(4, 1)$.

5. Des carrés d'indices élevés

P. Ribemboin et W. Mc Daniel ([3]) ont montré que si V_n ou U_n est un carré, ou le double d'un carré, alors $n \leqslant 12$. Il n'en est pas ainsi pour les suites (x_n) plus générales considérées ici.

On utilise la formule

$$x_n = U_n x_1 - QU_{n-1}x_0 \tag{7}$$

vraie pour $n = 1$ ($U_1 = 1$, $U_0 = 0$), pour $n = 2$ ($U_2 = P$) et donc pour tout n car ses deux membres satisfont la même formule de récurrence.

Comme $u_{k+1} \equiv PU_k \mod Q$ et comme P est premier à Q, on voit que U_n est premier à Q pour tout n. D'autre part (7) appliqué à (V_n) donne $V_n = U_nP - 2QU_{n-1}$ de sorte qu'un diviseur premier commun à U_n et QU_{n-1} doit diviser V_n et donc $V_n^2 - DU_n^2 = 4Q^n$, impossible. Donc U_n et QU_{n-1} sont premiers entre eux de sorte que, pour n et c donnés, on peut trouver des entiers x_0 et x_1 tels que $c = U_n x_1 - QU_{n-1}x_0$.

Encore faut-il que x_0 et x_1 soient positifs et débutent une suite à termes positifs, c'est à dire que $x_1/x_0 > \beta$ (cf. § 1). Comme x_0 est déterminé modulo U_n, on peut supposer que $0 < x_0 \leqslant U_n$. Alors on a $x_1/x_0 = (c + QU_{n-1}x_0)/U_n x_0$; comme $f(t) = (c + QU_{n-1}t)/U_n t$ est décroissante, on

a $x_1/x_0 \geqslant (c + QU_{n-1}U_n)/U_n^2$ et il suffit d'un carré c tel que :

$$c > \beta U_n^2 - QU_{n-1}U_n. \tag{8}$$

Remarque. On peut majorer le second membre de (8), notons le $U_n r_n$, par un nombre plus commode à calculer. En effet, comme $r_n = \beta U_n - QU_{n-1}$. la suite (r_n) satisfait notre relation de réccurence. Or on a $r_1 = \beta$, $r_2 = P\beta - Q = \beta^2$, $r_3 = P\beta^2 - Q\beta = \beta^3$,...,$r_n = \beta^n$. Ainsi (8) s'écrit $c > U_n\beta^n$.

D'autre part on a $U_n < \alpha^n$. En effet, de $\alpha^2 = P\alpha - Q$, d'où $\alpha^{n+1} = P\alpha^n - Q\alpha^{n-1}$, on déduit que la suite $s_n = \alpha^n - U_n$ satisfait notre relation de récurrence. Or $s_0 = 1$, $s_1 = \alpha - 1 = \frac{1}{2}(P - 2 + \sqrt{D}) > \frac{1}{2}(P - \sqrt{D})$ (car $\sqrt{D} > 1$). D'où $s_1/s_0 > \beta$ et la suite (s_n) est à termes positifs. Ainsi $U_n\alpha^n$ est majoré par $\alpha^n\beta^n = Q^n$ et il suffit de prendre $c \geqslant Q^n$. Par exemple $c = (Q^8)^2$ pour $n = 16$.

6. Suites contenant trois carrés

Par translation, on peut supposer que les indices de ces trois carrés dans une suite (x_n) sont 0, j, k. Or on a $U_j x_k = U_k x_j - Q^j U_{k-j} x_0$. Pour k fixé, c'est vrai pour $j = 0$, pour $j = 1$ par (7) et donc pour tout j car les deux membres satisfont la même relation de récurrence (noter que $Q^j U_{k-j} = -U_{j-k}$).

Il s'agit donc, d'abord, de voir si une équation de la forme

$$az^2 = by^2 - cz^2 \tag{9}$$

a des solutions (entières, bien sûr) non triviales. C'est un problème classique (cf. [4], Chap. IV). La condition de possibilité est, ici, facile à écrire. En multipliant par a et en mettant en évidence les parties sans facteurs carrés, on écrit $(az)^2 = b'(b''y)^2 - c'(c''x)^2$ avec b', c' sans facteurs carrés. En multipliant une solution (x', y', z') de $z'^2 = b'y'^2 - c'x'^2$ par un entier convenable, on trouve une solution de (9). Or, pour que $z'^2 = b'y'^2 - c'x'^2$ ait une solution non triviale il faut que

$$b' \text{ est un carré modulo } c' \text{ et } -c' \text{ est un carré modulo } b'. \tag{10}$$

Mais, par une démonstration essentiellement dûe à Legendre ([4], pp. 73–75), cette condition est aussi suffisante.

Etant donnée une solution (x, y, z) de (9), reste à voir si la suite (x_n), $x_k = z^2$, $x_j = y^2$ et $x_0 = x^2$ a tous ses termes positifs. Comme dans le § 5, cela se traduit par une inégalité portant sur x^2, y^2, z^2 (y^2/x^2 "grand" dans le cas du § 5). Or les points rationnels de la conique projective d'équation (9) sont denses dans l'ensemble des points réels (couper celle–ci par les droites de pente rationnelle passant par un point rationnel donné). L'inégalité peut donc être satisfaite.

Exemple. Dans le cas de 3 carrés consécutifs, supposons P et Q premiers. L'équation est $z^2 = Py^2 - Qx^2$. La premiere condition (10), $(\frac{P}{Q}) = 1$, implique la seconde $(\frac{-Q}{P}) = 1$ sauf si on a $P \equiv -1 \mod 4$ et $Q \equiv 1 \mod 4$. Elles sont vraies pour $(P, Q) = (7, 3)$ (solutions $(x, y, z) = (1, 1, 2)$, $(1, 2, 5)$, ...), pour $(P, Q) = (11, 7)$ (solutions $(x, y, z) = (1, 1, 2)$, $(5, 11, 34), \ldots$), pour $(P, Q) = (11, 19)$ (solutions $(x, y, z) = (1, 2, 5)$, $(1, 5, 16), \ldots$). Aucune autre paire (P, Q) avec $P = 5$, 7, 11 ne convient.

Notes.

(1) Cette façon commode de définir les nombres U_n et V_n et de calculer avec eux n'est, en toute rigueur, valable que si D n'est pas un carré (c'est le cas si P et Q sont impairs car alors $D = P^2 - 4Q \equiv 5 \mod 8$). Sinon on part des définitions rébarbatives $V_n = \alpha^n + \beta^n$ et $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ et le formulaire reste vrai (on peut invoquer "la généralité de l'algèbre" : approcher p-adiquement un couple (P, Q) tel que $P^2 - 4Q$ est un carré par des couples (P', Q') tel que $P'^2 - 4Q'$ n'en soit pas un).

(2) (sur les périodes) a) Un petit calcul donne

$$x_6 = P(P^4 - 4P^2Q + 3Q^2)x_1 + (3P^2Q^2 - P^4Q - Q^3)x_0.$$

Avec P et Q impairs, on voit, modulo 8, que $P^4 - 4P^2Q + 3Q^2 \equiv 4(1 - Q) \equiv 0$. D'autre part, $3P^2Q^2 - P^4Q - Q^3 \equiv 3 - 2Q \mod 8$ et l'on a $3 - 2Q \equiv 1 \mod 8$ si $Q \equiv 1 \mod 4$ et $3 - 2Q \equiv 5 \mod 8$ si $Q \equiv -1 \mod 4$. Donc x_6 est congru à x_0 ou $5x_0$ modulo 8. Par décalage des indices, x_7 est congru à x_1 ou $5x_1$, etc.

Donc, si $Q \equiv -1 \mod 4$, on a $x_{12} \equiv 5x_6 \equiv 25x_0 \equiv x_0 \mod 8$ et la suite (x_n) a période 12.

Si $Q \equiv 1 \mod 4$, la période est 6. Les formules $x_{n+6} + Q^3 x_n = V_3 x_{n+3}$ et $V_3 = P(P^2 - 3Q)$ montrent que, pour tout diviseur premier impair p de $P^2 - 3Q$, on a $(\frac{x_{n+6}}{p}) = (\frac{-Q}{p})(\frac{x_n}{p})$ et $(\frac{3Q}{p}) = 1$, d'où $(\frac{x_{n+6}}{p}) = (\frac{-3}{p})(\frac{x_n}{p})$. Comme $Q \equiv 1 \mod 4$, on a $P^2 - 3Q \equiv -2 \mod 8$ et l'on peut écrire $P^2 - 3Q = 2s$ avec s impair. De plus, si P est premier à 3, on a $2s \equiv 1 \mod 3$, $s \equiv -1 \mod 3$ de sorte que $P^2 - 3Q$ admet un diviseur premier $p \equiv -1 \mod 3$. Alors la Loi de Réciprocité montre facilement que $(\frac{-3}{p}) = -1$. D'où, $(\frac{x_{n+6}}{p}) = -(\frac{x_n}{p})$. Ainsi, si x_a est un carré modulo p (p.ex. si x_a est un carré), alors aucun $x_{a+6+12k}$ ne peut être un carré.

Pour $(P, Q) = (7, 5)$, on a $P^2 - 3Q = 34$ et le nombre p vaut 17. Si P est un multiple de 3, un tel diviseur $p \equiv -1 \mod 3$ n'existe pas nécessairement : pour $(P, Q) = (15, 13)$, on a $P^2 - 3Q = 2 \cdot 3 \cdot 31$ et 31 ne convient pas ; mais, pour $(P, Q) = (15, 17)$, on a $P^2 - 3Q = 2 \cdot 3 \cdot 29$ et $p = 29$ convient.

b) Modulo 5, on rencontre, pour $(\frac{x_n}{5})$, des périodes 3, 4, 10 et 12. Cette période peut dépendre des termes initiaux x_0 et x_1. Constatations analogues modulo 3.

c) Pour un diviseur premier p de P (resp. q de Q), la période de $(\frac{x_n}{p})$ (resp. $(\frac{x_n}{q})$) peut être 1, 2 ou 4 (resp. 1 ou 2) selon les valeurs $(\frac{-Q}{p})$ (resp. $(\frac{P}{q})$) et des termes initiaux.

(3) Lorsque x_a est un multiple de tous les diviseurs premiers $p \equiv -1 \mod 4$ de V_6 (et si A) ne s'applique pas), on doit soumettre x_a et x_{a+12} (ou x_{a-12} au test V_{12}.

(4) Des raisons de probabilités laissent deviner ce succès. Par exemple, si V_6 (ou V_{12}) a un diviseur $q \equiv 1 \mod 4$ et deux diviseurs premiers p, $p' \equiv -1 \mod 4$, les "mauvais" cas B.2) et B.3) ont lieu lorsque les Symboles de Legendre valent $(1, 1, 1)$ et $(1, -1, -1)$; leur probabilité est $1/4$, tandis que les "bons" cas A) et B.1) ont probabilité $3/4$.

Mais il n'y a pas de borne pour le nombre de tests à effectuer. Prenons pour x_0 un non-carré qui est un carré modulo tous les diviseurs premiers de $V_6, V_{12}, \ldots, V(3 \cdot 2^j)$ et aussi modulo 8, P, Q, 5, 3, 9. Dans tous les tests jusqu'à $V(3 \cdot 2^j)$ on est dans le "mauvais" cas B.2) et il faut continuer.

D'autre part, si $Q = 1$, la formule $V_{2n} = 2V_n^2 - 1$ montre que 2 est un carré modulo V_{2n}, en particulier V_6, V_{12}, $V_{24}, \ldots$ Donc, si le terme x_a à tester est de la forme $2k^2$, on se trouve indéfiniment dans le cas B.2) et, par éliminations successives des indices $a + 12 + 24q$, $a + 24 + 48q, \ldots$, aucun x_{a+12j} n'est un carré.

(5) J'ai travaillé au cas-par-cas, avec des moyens de calcul rudimentaires. Un programme d'ordinateur permettrait certainement d'aller plus loin (il en existe pour les équations Diophantiennes du § 4, qui reviennent à la recherche des points entiers de courbes elliptiques). J'espère que l'on pardonnera à un octogénaire de ne pas l'avoir fait et d'avoir préféré occuper ses loisirs à "jouer avec des nombres".

Bibliographie

[1] J.H.E. Cohn, *Eight Diophantine equations*. Proc. London Math. Soc. (3), **16** (1966), 153–166.

[2] J.H.E. Cohn, *Some quartic Diophantine equations*. Pacific J. of Math. **26, 2** (1968), 233–243.

[3] W. Mc Daniel, P. Ribenboim, *The square terms in Lucas sequences*. J. Number Theory, **58, 1** (1996), 104–123.

[4] J.P. Serre, *Cours d'Arithmétique*. Presses Univ. de France, 1970.

Pierre Samuel
3, Avenue du Lycée Lakanal
92340 Bourg-La-Reine