

MAURICE MIGNOTTE

ATTILA PETHÖ

Sur les carrés dans certaines suites de Lucas

Journal de Théorie des Nombres de Bordeaux, tome 5, n° 2 (1993),
p. 333-341

http://www.numdam.org/item?id=JTNB_1993__5_2_333_0

© Université Bordeaux 1, 1993, tous droits réservés.

L'accès aux archives de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

Sur les carrés dans certaines suites de Lucas

par MAURICE MIGNOTTE ET ATTILA PETHŐ

ABSTRACT – Let a be an integer ≥ 3 . If $\alpha = (a + \sqrt{a^2 - 4})/2$ and $\beta = (a - \sqrt{a^2 - 4})/2$, we consider the Lucas sequence $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. We prove that for $a \geq 4$, u_n is neither a square, nor a double or a triple square, nor six times a square for $n > 3$, except for $a = 338$ and $n = 4$.

RÉSUMÉ – Soit a un entier ≥ 3 . Pour $\alpha = (a + \sqrt{a^2 - 4})/2$ et $\beta = (a - \sqrt{a^2 - 4})/2$, nous considérons la suite de Lucas $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$. Nous montrons que, pour $a \geq 4$, u_n n'est ni un carré, ni le double, ni le triple d'un carré, ni six fois un carré pour $n > 3$, sauf si $a = 338$ et $n = 4$.

1 Énoncé des résultats

Soient a et b deux entiers non nuls premiers entre eux. On suppose $\Delta = a^2 - 4b > 0$ et on pose

$$\alpha = \frac{a + \sqrt{\Delta}}{2}, \quad \beta = \frac{a - \sqrt{\Delta}}{2}, \quad u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad v_n = \alpha^n + \beta^n \quad (n \text{ entier } \geq 0).$$

Récemment, McDaniel et Ribenboim [1] ont étudié les carrés et les doubles de carrés parmi les valeurs des suites u et v . Ils ont démontré des résultats très précis qui impliquent en particulier l'énoncé suivant.

THÉORÈME A. *Si a et b sont impairs et premiers entre eux et si u_n est un carré ou le double d'un carré alors $n \leq 12$.*

Dans ce travail, nous ne considérons que le cas où $b = 1$, mais nous supposons a quelconque et nous démontrons le résultat suivant.

THÉORÈME. *Soit a un entier ≥ 3 , tel que $\Delta = a^2 - 4$ ne soit pas le carré d'un entier. Nous posons $\alpha = (a + \sqrt{a^2 - 4})/2$ et $\beta = (a - \sqrt{a^2 - 4})/2$, et nous considérons la suite de Lucas $u_n = u_n(a) = (\alpha^n - \beta^n)/(\alpha - \beta)$. Alors,*

pour $a \geq 4$, u_n n'est ni un carré, ni le double, ni le triple d'un carré, ni six fois un carré pour $n > 3$, sauf si $a = 338$ et $n = 4$.

2 Etude de certaines unités

Soit γ un entier algébrique dont les conjugués sont $\gamma = \gamma_1, \gamma_2, \dots, \gamma_d$, on pose $M(\gamma) = \prod_{k=1}^d \max\{1, |\gamma_k|\}$.

LEMME 1. Soit γ un entier algébrique de degré d , alors le discriminant D de l'ordre $\mathbb{Z}[\gamma]$ vérifie

$$|D| \leq d^d M(\gamma)^{2(d-1)}.$$

Démonstration. En effet,

$$|D| \leq \text{Discr}(1, \gamma, \gamma^2, \dots) = \det^2 \begin{pmatrix} 1, \gamma_1, \gamma_1^2, \dots, \gamma_1^{d-1} \\ 1, \gamma_2, \gamma_2^2, \dots, \gamma_2^{d-1} \\ \dots \\ 1, \gamma_d, \gamma_d^2, \dots, \gamma_d^{d-1} \end{pmatrix},$$

et la conclusion résulte de l'inégalité de Hadamard. **CQFD**

Les racines du polynôme $X^2 - aX + 1$ sont α et β . On définit le nombre algébrique complexe $\theta = \sqrt{-\alpha\sqrt{\Delta}}$. Les conjugués de θ sont $\theta, -\theta, \theta_1 = \sqrt{\beta\sqrt{\Delta}}$ et $-\theta_1$. Le corps $K = \mathbb{Q}(\theta)$ est un corps quartique qui admet exactement deux plongements réels. Le rang du groupe de ses unités est donc égal à 2. On remarque que α et $\varepsilon = 1 + \theta$ sont des unités de K .

Montrons d'abord que pour $a \geq 4$, α est une unité fondamentale de l'ordre $\mathbb{Z}[\alpha]$. On a $\text{Discr } \mathbb{Z}[\alpha] = a^2 - 4$, et si $\alpha = \omega^k, \omega \in \mathbb{Z}[\alpha], k > 0$, alors $\text{Discr } \mathbb{Z}[\omega] = \omega^2 + \omega^{-2} \pm 2 < a^{2/k} + a^{-2/k} + 2$; ce qui impose $k = 1$ pour $a \geq 4$.

Notons $x \mapsto x' = \bar{x}, x \mapsto x_1$ et $x \mapsto x'_1$ les plongements de K dans \mathbb{C} qui envoient respectivement θ sur $-\theta, \theta_1$ et $-\theta_1$. Si $\alpha = \omega^k, \omega \in R = \mathbb{Z}[\theta], k \geq 2$, alors $\omega\omega'$ est une unité de $\mathbb{Z}[\alpha]$ et donc $k = 2$; mais, comme les quatre conjugués de $\sqrt{\alpha}$ sont réels, ceci est impossible. Donc, en appliquant le théorème 7.1, chapitre 5, de [2], on conclut que α appartient à un système fondamental d'unités de R .

Nous allons montrer que $\{\alpha, \varepsilon\}$ est un système fondamental d'unités de R . D'après [2], chapitre 5, théorème 7.1, il suffit de montrer que l'équation $\varepsilon^{-1} = \alpha^h \omega^k$ n'a pas de solution $\omega \in R$, avec $0 < h < k$. Une telle relation implique $(\varepsilon\varepsilon')^{-1} = \beta^2 = \alpha^{2h}(\omega\omega')^k$, avec $\omega\omega' = \alpha^{-u}$. Donc $uk = 2(h + 1)$,

et $u = 1$ ou 2 . Dans les deux cas, ceci conduit à $\alpha\varepsilon^{-1} = \xi^\ell$, $\ell \geq 2$, où $\xi \in R$.

On vérifie que $M(\alpha/\varepsilon) = \beta/(1 - \theta_1) = \alpha(1 + \theta_1) < 2a$. Et,

$$|\text{Discr}(R)| = a^4(16a^6 - 192a^4 + 768a^2 - 1024) \geq 107a^6, \quad \text{pour } a \geq 4.$$

Le lemme 1 permet de montrer que $\ell < 2$. D'où le résultat.

3. Réduction au cas d'un indice impair

Remarquons d'abord que si a est impair, alors u_n pair équivaut à n divisible par 3, tandis que si a est pair, on a $u_n \equiv n \pmod 2$.

LEMME 2. *Soit $p \geq 5$ un nombre premier. Alors, tout diviseur premier de u_p est supérieur ou égal à p . De plus, si $p|u_p$ alors p divise Δ .*

Démonstration. Supposons que q soit un nombre premier, $q \nmid \Delta$. Comme $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ et que $\alpha\beta = 1$, le fait que q divise u_n équivaut à la condition $\alpha^{2n} \equiv 1 \pmod q$. Il en résulte que, pour p premier ≥ 5 , si q divise u_p alors q ne divise pas u_n pour $0 < n < p$.

Par ailleurs, le corps fini $\mathbb{F}_q(\alpha)$ est égal à \mathbb{F}_q lorsque $\binom{\Delta}{q} = +1$ et à \mathbb{F}_{q^2} lorsque $\binom{\Delta}{q} = -1$. Dans le premier cas, si $q|u_p$ alors, comme $\alpha^{q-1} \equiv 1 \pmod q$, on a $p|(q-1)$. Dans le second cas, on a $\alpha^{p+1} = \alpha^p\alpha = \beta\alpha = 1 \pmod q$ et donc $p|(q+1)$. Donc, dans les deux cas $q > p$.

Si $p|u_p$ alors p divise Δ (d'ailleurs, si $p|\Delta$, on a $u_n \equiv \pm n \pmod p$ et donc $p|u_p$). **CQFD**

On notera par \square le carré d'un entier non nul et par $w_p(x)$ la valuation p -adique de l'entier x .

LEMME 3. *Soit m un entier dont le plus grand diviseur premier est $q > 3$. Si $u_m = \square$ ou $2\square$ ou $3\square$ ou $6\square$, alors $u_q = \square$ ou $u_{q^2} = \square$.*

Démonstration. Soit m un entier dont le plus grand diviseur premier est $q > 3$ et tel que $u_m = \square$ ou $2\square$ ou $3\square$ ou $6\square$.

D'après la remarque qui précède le lemme 2, u_q est impair. De plus $u_q|u_m$. Soit r un diviseur premier de u_q , d'après le lemme 2, $r \geq q$. La preuve du lemme 2 montre que si $r|u_n$ alors $q|n$. Soit $s = w_r(u_q)$. Supposons que $r^{s+1}|u_n$ et posons $n = qn'$. Alors, si $r \nmid \Delta$, on a $r > q$, et la congruence

$$\alpha^{2n} = (\alpha^{2q})^{n'} = (1 + r^s\alpha')^{n'} \equiv 1 + n'r^s\alpha' \pmod{r^{s+1}},$$

où $r \nmid \alpha'$, montre que $r^{s+1} | u_n$ si, et seulement si, $rq | n$. On a donc $w_r(u_m) = s$, s pair. Il s'ensuit que u_q est un carré si $q \nmid \Delta$.

Reste le cas où $q | \Delta$ et où u_q n'est pas un carré. Alors $w_q(u_q)$ est impair, $\alpha^q \equiv \beta^q \pmod{q\sqrt{\Delta}}$ et

$$u_{q^2} = u_q (\alpha^{q(q-1)} + \alpha^{q(q-2)}\beta^q + \dots + \beta^{q(q-1)}) \equiv u_q q \alpha^{q(q-1)} \pmod{qu_q \sqrt{\Delta}},$$

donc $w_q(u_{q^2}) = 1 + w_q(u_q)$ est pair. Les autres diviseurs de u_{q^2} sont strictement supérieurs à q et l'argument précédent montre que u_{q^2} est un carré. **CQFD**

LEMME 4. *Soient $a \geq 3$ et $m = 2^s 3^t$ avec $s, t \geq 0$ et $s + t \geq 2$. Il existe alors un nombre premier $p \geq 5$ tel que $w_p(u_m)$ soit impair, excepté pour $a = 338$, $m = 4$ et $u_m = 6214^2$ et pour $a = 3$ et $m = 6$, auquel cas $u_m = 12^2$.*

Démonstration. Plus tard, nous démontrerons que l'assertion est vraie pour $m = 4, 6$ et 9 . Supposons qu'elle soit vraie pour toutes les paires (s, t) avec $2 \leq s + t < S$. Soient s et t tels que $s + t = S$ et soit $m = 2^s 3^t$. Si $s > 0$, soit $m' = m/2$, sinon soit $m' = m/3$. Dans le premier cas, $u_m = u_{m'} v_{m'}$, tandis que $u_m = u_{m'}(v_{m'}^2 - 1)$ dans le second cas. Par hypothèse, il existe p premier > 3 avec $w_p(u_{m'})$ impair. Comme $(u_{m'}, v_{m'}) = 1$ ou 2 et $(u_{m'}, v_{m'}^2 - 1) = 1$ ou 3 , on a $w_p(u_m) = w_p(u_{m'})$ et l'assertion est démontrée.

Considérons d'abord le cas $m = 4$. Notons que $u_4 = a(a^2 - 2)$ et $v_4 = a^4 - 4a^2 + 2$.

Si $u_4 = \square$ alors $a(a^2 - 2) = \square$. Si a est impair, $(a, a^2 - 2) = 1$ et $a^2 - 2 = \square$, ce qui est impossible. Si a est pair alors $a = 2x^2$, $a^2 - 2 = 2y^2$, donc $2x^4 - 1 = y^2$, et Ljungreen [3] a montré que ceci implique $(x, y) = (1, 1)$ ou $(13, 239)$. Donc $a = 338$. On a toujours $v_4 \neq \square$, de plus $v_4(338) \neq 2\square$, donc $u_m(338) \neq \square$ et $\neq 2\square$ pour $s > 2$. On constate que $w_{113}\{u_{12}(338)\} = w_{9601}\{u_8(338)\} = 1$.

Si $u_4 = 2\square$, a doit être pair. Et on a $a \neq \square$, $a^2 - 2 = 2\square$, soit $a = 4x^2$ et $16x^4 - 2 = 2y^2$: impossible modulo 8.

Si $u_4 = 3\square$ ou $6\square$ alors $3|a$ et $a^2 - 2 = \square$ ou $2\square$. Il est clair que la première relation est impossible, et la seconde est impossible modulo 9. D'où le résultat pour $m = 4$.

Supposons maintenant que $u_9 = \square, 2\square, 3\square$ ou $6\square$. Il est facile de voir que

$$u_9 = u_3(v_3^2 - 1) = (a^2 - 1)(a^3 - 3a + 1)(a^3 - 3a - 1),$$

où le nombre $v_3^2 - 1$ est toujours impair.

Si $3|a$ alors $(u_3, v_3^2 - 1) = 1$ et $3 \nmid u_9$, donc, si $u_9 = \square$ alors $u_3 = \square$ et si $u_9 = 2\square$ alors $v_3^2 - 1 = \square$, ces deux cas sont donc impossibles.

Si $a \equiv 1 \pmod 3$ alors $(u_3, v_3^2 - 1) = 3$ et ni 2, ni 3 ne divisent $a^3 - 3a + 1$ et $a^3 - 3a + 1 = \square$ est impossible modulo 3, il existe donc p premier > 3 avec $w_p(a^3 - 3a + 1) = w_p(u_9)$ impair.

Si $a \equiv -1 \pmod 3$ alors $(u_3, v_3^2 - 1) = 3$ et ni 2 ni 3 ne divisent $a^3 - 3a - 1$. On a $a^3 - a + 1 = 3\square$, $a^3 - a - 1 = \square$ et $a^2 - 1 = 2\square$ ou $3\square$ ou $6\square$.

Si $a^2 - 1 = 2\square$ alors $a = a_k$ où $a_0 = 1$, $a_1 = 3$ et $a_{k+2} = 6a_{k+1} - a_k$ pour $k \geq 0$, ce qui impose $a \equiv 1 \pmod 4$ lorsque $a \equiv -1 \pmod 3$. Mais, puisque $a \equiv 1 \pmod 4$, on a $\binom{3}{a} = \binom{3}{3} = \binom{-1}{3} = -1$: contradiction.

Si $a^2 - 1 = 6\square$ alors $a = a_k$ où $a_0 = 1$, $a_1 = 5$ et $a_{k+2} = 10a_{k+1} - a_k$ pour $k \geq 0$, donc $a \equiv 1 \pmod 4$: contradiction déjà vue.

Si $a^2 - 1 = 3\square$ alors $a = a_k$ où $a_0 = 1$, $a_1 = 2$ et $a_{k+2} = 4a_{k+1} - a_k$ pour $k \geq 0$, ainsi $a \equiv 2 \pmod 4$ lorsque $a \equiv -1 \pmod 3$. Donc $(a-1, a+1) = 1$ et $a - 1 = t^2$. Comme $a^3 - a - 1 = \square$, on a

$$(t^2 + 1)^3 - 3(t^2 + 1) - 1 = t^6 + 3t^3 - 3 = z^2,$$

ce qui impose $t^3 z < t^3 + 1$ et la seule solution est $t = 1$, ce qui correspond à $a = 2$ et $u_9 = 9$ (cas exclu, puisque $a \geq 3$).

Enfin, supposons que $u_6 = \square, 2\square, 3\square$ ou $6\square$. Notons que $u_6 = u_3 v_3$ et $u_3 = a^2 - 1, v_3 = a(a^2 - 3)$ avec $(u_3, v_3) = 1$ ou 2.

Si $u_6 = \square$ alors $u_3 = 2\square$ et $v_3 = 2\square$. Donc a impair, $a^2 - 1 = 2x^2$, $a(a^2 - 3) = 2y^2$. Ce qui donne $a = 3z^2$ et $a^2 - 3 = 6t^2$. D'où les conditions $9z^4 - 1 = 2x^2$ et $9z^4 - 3 = 6t^2$. On a la solution évidente $z = 1$, le lemme 5 ci-dessous montre que c'est la seule. Ainsi, $a = 3$. On constate que $w_7\{u_{12}(3)\} = w_{17}\{u_{18}(3)\} = 1$.

Si $u_6 = 2\square$ alors $u_3 v_3 = 2\square$, avec $u_3 \neq \square$, donc $v_3 = \square, u_3 = 2\square$ et a impair. Comme $v_3 = a(a^2 - 3)$ avec a impair, on a $v_3 \equiv \pm 2 \pmod 4$, en contradiction avec $v_3 = \square$.

Restent les cas $u_6 = 3\square$ ou $6\square$.

$v_3 = \square$ est impossible. En effet, dans ce cas $3|u_3$, ainsi $3 \nmid a$ et donc $3 \nmid v_3$. Donc $a = \square$ et $a^2 - 3 = \square$ (soit $a = 2$) : contradiction.

$u_3 = \square$ est impossible.

$v_3 = 2\Box$, $u_3 = 3\Box$ ou $u_3 = 6\Box$ ne peuvent avoir lieu que pour $a = 2$. En effet $3 \nmid a$, et donc $a^2 - 3 = \Box$ ou $2\Box$. La première équation donne $a = 2$, la seconde est impossible modulo 3.

$u_3 = 2x^2$, $v_3 = 3\Box$ ou $6\Box$. Alors a est impair et divisible par 3. Donc $w_3(a^2 - 3) = 1$ et $a = y^2$. On aboutit à l'équation $y^4 - 2x^2 = 1$ qui, d'après Ljungreen [3], ne possède que la solution triviale $y = 1$. On constate que $w_7\{u_{12}(3)\} = 1$ et que $u_{18} = u_6(v_6^2 - 1) = u_6 \times 103683$, où $103683 = 3 \times 17 \times 19 \times 107$. Ce qui achève la démonstration, du lemme. **CQFD**

LEMME 5. *Le système d'équations en nombres entiers positifs*

$$3Z^2 - 1 = 2Y^2 \quad \text{et} \quad 9Z^2 - 1 = 2X^2$$

n'a que la solution banale $Z = 1$.

Démonstration. Supposons X , Y et Z positifs. La première équation implique $(2Y)^2 - 6Z^2 = 2$ et comme $2 = (2 + \sqrt{6})^2(5 - 2\sqrt{6})$, on en déduit l'existence d'un entier $s \geq 0$ tel que $\sqrt{6}Z + 2Y = (2 + \sqrt{6})(5 + 2\sqrt{6})^s$. La seconde relation implique l'existence d'un entier positif t tel que $3Z + \sqrt{2}X = (3 + 2\sqrt{2})^t$. Donc

$$\begin{aligned} Z &= \frac{(2 + \sqrt{6})(5 + 2\sqrt{6})^s - (2 - \sqrt{6})(5 - 2\sqrt{6})^s}{2\sqrt{6}} \\ &= \frac{(3 + 2\sqrt{2})^t + (3 - 2\sqrt{2})^t}{6}. \end{aligned}$$

Il en résulte que la quantité

$$\Lambda = s \log(5 + 2\sqrt{6}) - t \log(3 + 2\sqrt{2}) + \log(3 + \sqrt{6})$$

vérifie

$$|\Lambda| \leq (\sqrt{6} - 2)^{-2}(5 + 2\sqrt{6})^{-2s} + (3 + 2\sqrt{2})^{-2t}.$$

On en déduit

$$s \log(5 + 2\sqrt{6}) < t \log(3 + 2\sqrt{2}) < (s + 1) \log(5 + 2\sqrt{6})$$

donc $t > s$ et

$$|\Lambda| < (3 + 2\sqrt{2})^{-2t} \left(1 + (5 + 2\sqrt{6})^2 (\sqrt{6} - 2)^2 \right) < 21(3 + 2\sqrt{2})^{-2t}.$$

Une application de l'estimation de M. Waldschmidt [5] fournit la borne $t \leq 10^{21}$. Ensuite, on procède comme Baker et Davenport en [4] : une première application du lemme ci-dessous avec $q = 337472905923410699064273181$ conduit à la nouvelle borne $t \leq 30$. En choisissant cette fois $q = 264$ on trouve $t \leq 4$. Puis on vérifie que la seule solution est $t = 1$, d'où $Z = 1$. **CQFD**

LEMME 6 (Baker-Davenport, [5]). Soit $\varphi = a_1\xi_1 + \xi_2 + a_2$, où les a_i sont entiers, $0 < a_1 < B$, et les ξ_i réels, tel que $|\varphi| < e^{-\lambda a_1}$, $\lambda > 0$. Soit q un entier positif tel que $|q\varphi| < 1/q$ et $\varepsilon = ||q\xi_2|| - B/q > 0$, alors $a_1 \leq \log(q/\varepsilon)/\lambda$, (où $||x||$ est la distance à l'entier le plus proche).

4 Démonstration du théorème

Supposons que le nombre $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$ soit le carré d'un entier x , alors $\alpha^{n+1} = \alpha\sqrt{\Delta}x^2 + \alpha\beta^n$. Lorsque n est impair ≥ 5 , $n = 2m + 1$ avec $m \geq 2$, et cette relation implique

$$\alpha^{2(m+1)} = (\theta x + \beta^m)(-\theta x + \beta^m),$$

donc $\theta x + \beta^m$ est une unité. D'où l'existence d'entiers u et v , $v > 0$, tels que

$$\begin{aligned} \theta x + \beta^m &= \beta^u \varepsilon^v, \quad -\theta x + \beta^m = \beta^u \bar{\varepsilon}^v, \quad \theta_1 x + \alpha^m = \alpha^u \varepsilon_1^v \\ &\text{et} \quad -\theta_1 x + \alpha^m = \alpha^u \varepsilon_1'^v. \end{aligned}$$

De ces relations, il vient

$$2\theta\theta_1 x = \theta_1 \beta^u (\varepsilon^v - \bar{\varepsilon}^v) = \theta \alpha^u (\varepsilon_1^v - \varepsilon_1'^v), \quad 2\alpha^m (\theta x + \beta^m) = \varepsilon^v (\varepsilon_1^v + \varepsilon_1'^v),$$

donc, compte tenu de la formule $x^2 = (\alpha^n - \beta^n)/(\alpha - \beta)$,

$$(*) \quad \left| \log 2 + (2m + 1) \log \alpha - v \log |\varepsilon \varepsilon_1| \right| < 1/a.$$

Par ailleurs, il existe un entier k tel que

$$\Lambda = v \log(\varepsilon/\bar{\varepsilon}) - ik\pi$$

vérifie $|\Lambda| \leq 4\beta^{2m}$, donc

$$|\Lambda| < 9a|\varepsilon \varepsilon_1|^{-v}.$$

Mais, en utilisant les résultats de [6], on obtient la minoration

$$|\Lambda| \geq \exp(-270 \times 2^4 \times \log(a^2) \times (7.5 + \log v)^2).$$

Il en résulte que $v \leq V = 4,6 \times 10^6$. En développant $\log(\varepsilon/\bar{\varepsilon})$, on obtient

$$\Lambda = i\pi \left(v - \frac{2v}{\pi} \left(\frac{1}{|\theta|} - \frac{1}{3|\theta|^3} + \frac{1}{5|\theta|^5} - \dots \right) - k \right).$$

On voit que pour $v = k$ on a $|\Lambda| \geq 1/(2a)$, ce qui contredit la majoration précédente de $|\Lambda|$; on a donc $v > k$, ce qui implique $v > \pi(a - 2)/2$. Donc $a < 2 + 2v/\pi < 2,910^6$.

Pour $a > 800000$, on a $1 \leq v - k \leq 3$ et on vérifie rapidement (sur ordinateur) que la majoration $|\Lambda| < 9a|\varepsilon\varepsilon_1|^{-v}$. n'a pas lieu.

Un second calcul sur ordinateur montre que $|\Lambda| \geq a^{-3}v^{-2}$ pour $16 < a \leq 800000$ et $0 < v \leq V$. Pour ces valeurs de a , il s'ensuit que l'on a

$$a^{-3}v^{-2} < 9a|\varepsilon\varepsilon_1|^{-v},$$

ce qui implique $v \leq 6$, donc $a < 2 + 2v/\pi < 6$: contradiction.

Pour $4 \leq a \leq 16$, on a $|\Lambda| \geq 1/(2700v^2)$ si $0 < v \leq V$. D'où

$$(2700v^2)^{-1} < 9a|\varepsilon\varepsilon_1|^{-v},$$

soit $v \leq 11$, donc $a < 2 + 2v/\pi < 10$ et l'inégalité (*) donne $m \leq 10$; une vérification directe montre qu'il n'y a pas de solution.

Le théorème est alors une conséquence directe des lemmes 3 et 4.

Remarque : L'article [7] de Cusik contient le résultat suivant. Soit v_n la suite définie par les conditions $v_1 = 1$, $v_2 - 2 = k$ et $v_n = kv_{n-1} - v_{n-2}$, (c'est exactement notre suite u_n). Alors, pour $k > 2$, la suite v_n ne contient jamais deux carrés consécutifs, excepté lorsque k est un carré, auquel cas les seuls carrés consécutifs sont v_1 et v_2 . Ce résultat est une conséquence immédiate de notre théorème.

Remerciements : Nous sommes très reconnaissants au rapporteur grâce auquel de nombreux points ont été présentés plus clairement et qui nous a signalé une lacune dans la preuve du lemme 3 concernant l'étude du terme u_9 .

BIBLIOGRAPHIE

- [1] W. L. McDANIEL et P. RIBENBOIM, *Squares and double-squares in Lucas sequences*, C. R. Math. Rep. Acad. Sci. Canada **14** n° 2, 3 (1992), 104–108.
- [2] M. POHST & H. ZASSENHAUS, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.
- [3] W. LJUNGREEN, *Zur Theorie der Gleichung $x^2 + 1 = Dy^4$* , Avh. Norske Vid. Akad. Oslo, No. 5, 1, (1942).
- [4] A. BAKER et H. DAVENPORT, *The equations $3x^2 - 2 = y^2$ et $8x^2 - 7 = z^2$* , Quart. J. Math. Oxford **2** (1969), 129–137.

- [5] M. WALDSCHMIDT, *Minorations de combinaisons linéaires de logarithmes de nombres algébriques*, Canadian J. Math. **45** (1) (1993), 176–224.
- [6] M. MIGNOTTE et M. WALDSCHMIDT, *Linear forms in two logarithms and Schneider's method, III*, Annales Fac. Sci. Toulouse (1990), 43–75.
- [7] T. W. CUSIK, *The diophantine equation $x^4 - kx^2y^2 + y^4 = 1$* , Arch. Math. **59** (1992), 345–347.

Maurice Mignotte
Université Louis Pasteur
Département de mathématiques
7, Rue René Descartes
67084 –Strasbourg
FRANCE
e-mail : mignotte@math.u-strasbg.fr

Attila Pethő
Debreceni Orvostudományi Egyetem
Informatikai Laboratórium
4028–Debrecen Nagyerdei krt. 98.
HONGRIE
e-mail : h2988pet@ella.hu