SUR LES CARRÉS DANS CERTAINES SUITES DE FIBONACCI

Maurice MIGNOTTE (*)

Résumé.– Chacun connaît la suite de Fibonacci 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144... En 1964, J.H.E. Cohn a démontré que les seuls carrés de cette suite sont $0, 1$ et 144, démonstration que nous reproduisons au 1er paragraphe.

La suite de Fibonacci vérifie la récurrence $F_n = F_{n-1} + F_{n-2}$ pour $n \geq 2$. On considère ici les suites $u_n = u_n(a)$ définies par $u_0 = 0, u_1 = 1$ et $u_n = au_{n-1} - u_{n-2}$ pour $n \geq 2$, où a est un entier ≥ 3. (On notera que $u_n(3) = F_{2n}$.) Nous montrons que pour $a \geq 4$, alors 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 $n = 4$. Ce travail a été réalité en collaboration avec A. Pethö.

Dans toute la suite, on notera par $\square$ le carré d'un entier non nul. Les lettres p et q désigneront toujours des nombres premiers.

0.– Rappel sur les suites récurrentes linéaires sur deux termes

• On définit une telle suite par

$$\begin{cases} u_n = a\ u_{n-1} - b\ u_{n-2}, \text{ pour } n \geq 2, \\ u_0, u_1 \text{ donnés}, \end{cases}$$

a et b dans $\mathbb{C}$.

On démontre que si α et β sont les racines complexes de l'équation (dite équation caractéristique) $r^2 = ar - b$ alors l'ensemble des solutions est donné par :

a) si $\alpha \neq \beta$: $u_n = A\ \alpha^n + B\ \beta^n$, A et B étant obtenus à l'aide des conditions initiales $u_0 = A + B$ et $u_1 = A\alpha + B\beta$;

b) si $\alpha = \beta$: $u_n = (An + B)\alpha^n$, avec, pour les conditions initiales $u_0 = B$ et $u_1 = (A + B)\alpha$.

• Dans le cas particulier où a et b sont entiers : avec Δ, discriminant de l'équation caractéristique, positif ($a^2 - 4b > 0$) on a : $\alpha = \frac{a+\sqrt{\Delta}}{2}$ et $\beta = \frac{a-\sqrt{\Delta}}{2}$.

Si $u_0 = 0$ et $u_1 = 1$ on trouve alors $u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$. L'exemple fondamental est alors la suite de Fibonacci : $F_n = F_{n-1} + F_{n-2}$, $F_0 = 0$, $F_1 = 1$.

Si $u_0 = 2$ et $u_1 = a$ on trouve alors $u_n = \alpha^n + \beta^n$. L'exemple fondamental est alors la suite de Lucas : $L_n = L_{n-1} + L_{n-2}, L_0 = 2, L_1 = 1$.

(*) Conférence IREM de Strasbourg - Régionale APMEP d'Alsace donnée le 16 décembre 1992.

• Voici les premiers éléments de ces deux suites :

$$F_n : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 \ldots$$
$$L_n : 2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322 \ldots$$

Ces suites présentent des propriétés remarquables dont voici les plus utiles pour le présent article :

$$L_n^2 - 5F_n^2 = (-1)^n 4$$
$$L_{2m} - L_m^2 = (-1)^{m+1} 2$$
$$F_{2m} = F_m L_m$$
$$2L_{m+p} = 5F_m F_p + L_m L_p$$
$$2F_{m+p} = F_m L_p + L_m F_p$$

dont les démonstrations sont immédiates en remplaçant F_n et L_n par leur valeur respective $[(\frac{1+\sqrt{5}}{2})^n - (\frac{1-\sqrt{5}}{2})^n]\frac{1}{\sqrt{5}}$ et $[(\frac{1+\sqrt{5}}{2})^n + (\frac{1-\sqrt{5}}{2})^n]$. Ces formules permettent de donner un sens à F_n et L_n pour n négatif.

1.– Les suites de Fibonacci et Lucas

Nous allons d'abord montrer que les seuls carrés de la suite de Fibonacci (F_n) sont 0, 1 et 144 et que les seuls carrés de la suite de Lucas sont 1 et 4.

Modulo 4, ces deux suites sont de période 6 :

n	0	1	2	3	4	5	6	7	...
$F_n \bmod 4$	0	1	1	2	3	1	0	1	...
$L_n \bmod 4$	2	1	3	0	3	3	2	1	...

De la relation $L_n^2 - 5F_n^2 = (-1)^n 4$ et de la table ci-dessus, on déduit que

$$(F_n, L_n) = \begin{cases} 1, \text{ si } n \not\equiv \pmod 3, \\ 2, \text{ si } n \equiv \pmod 3. \end{cases}$$

a) Considérons d'abord la suite de Lucas. La relation $L_{2m} = L_m^2 - 2(-1)^m$ montre que L_n ne peut être un carré lorsque n est pair. Supposons donc n impair. On peut se limiter à $n > 0$, sinon L_n est négatif. On supposera de plus $n \geq 5$ (on notera que $L_1 = 1$ et $L_3 = 4$ sont des carrés). On peut écrire $n = c + 2tk$, avec $t = 3^r$, $k > 0$, $k \equiv \pm 2 \pmod 6$, ce qui prouve que k est pair, et enfin $c = 1$ ou 3. Les formules

$$2L_{m+2k} = 5F_m F_{2k} + L_m L_{2k} = 5F_m F_k L_k + L_m(L_k^2 - 2) \equiv -2L_m (\bmod\ L_k)$$

jointes au fait que L_k est impair [puisque $k \equiv \pm 2 \pmod 6$ implique $L_k \equiv 3 \pmod 4$] montrent que, par simplification par 2 :

$$L_n = L_{c+2tk} \equiv -L_c \equiv -1 \text{ ou } -4 \pmod{L_k}.$$

Si L_n est un carré, alors -1 est donc un carré modulo L_k, mais, comme $L_k \equiv 3$ modulo 4, ceci est impossible. Donc L_n ne peut être un carré pour $n \geq 5$.

b) Passons maintenant à la suite de Fibonacci.

• Si $n \equiv 1 \pmod 4$. Supposons $n \neq 1$ (sinon $F_n = 1$ est un carré). Comme plus haut, écrivons $n = 1 + 2tk$, avec $t = 3^r$ et $k \equiv \pm 2 \pmod 6$. Les formules

$$2F_{m+2k} = F_m L_{2k} + L_m F_{2k} = F_m(L_k^2 - 2) + F_k L_k L_m \equiv -2F_m \pmod{L_k}$$

et le fait que L_k est impair, impliquent

$$F_n \equiv -1 \pmod{L_k}.$$

Comme nous l'avons déjà vu, cette congruence implique que F_n n'est pas un carré.

• Si $n \equiv 3 \pmod 4$, le changement de n et $-n$ nous ramène au cas précédent.

• Si $n = 2m$ est pair, alors $F_n = F_m L_m = \square$ et on peut supposer $n > 0$.

• Si $m \not\equiv 0 \pmod 3$ on a $(F_m, L_m) = 1$ et donc $F_m = \square$ et $L_m = \square$, ce qui impose $m = 1$ ou 3; le seul carré pour F_n est 1.

• Si $m \equiv 0 \pmod 3$ on a $(F_m, L_m) = 2$ et donc $F_m = 2y^2$ et $L_m = 2z^2$. Si m est impair, on a $z^4 - 5y^4 = -1$, ce qui est impossible modulo 8. Si $m = 2m'$, alors $F_{m'} L_{m'} = 2y^2$. Si m' est impair, on a $F_{m'} = 2\square$ et $L_{m'} = \square$, donc $m' = 1$ ou 3; d'où $F_n = 1$ ou 144. Si m' est pair alors $F_{m'} = \square$ et $L_{m'} = 2\square$ ... On voit ainsi que les nombres de Fibonacci d'indices $n/4$, $n/16$... sont des carrés. Mais, comme F_6 et F_{48} ne sont pas des carrés, ce dernier cas est impossible. [Il n'est pas nécessaire de calculer F_{48} : si $F_{48} = \square$ alors $F_{24} = 2\square$, puis $L_{12} = 2\square$, mais $L_{12} = 322$.]

Nous avons donc démontré le résultat suivant dû à J.H.E. Cohn, [C].

THÉORÈME 1.– *Les seuls carrés de la suite de Fibonacci sont 0, 1 et 144, tandis que les seuls carrés de la suite de Lucas sont 1 et 4.*

2.– Énoncés des nouveaux résultats

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

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

Récemment, McDaniel et Ribenboim [McD-R] 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 2.– *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 $b = 1$ (1), mais nous supposons a quelconque et nous indiquons une méthode pour démontrer le résultat suivant.

THÉORÈME 3.– *Soit a un entier ≥ 3, et soit $\Delta = a^2 - 4$. Nous posons $\alpha = (a + \sqrt{\Delta})/2$ et $\beta = (a - \sqrt{\Delta})/2$, et nous considérons la suite de Fibonacci $u_n = u_n(a) = (\alpha^n - \beta^n)/(\alpha - \beta)$. 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 $n = 4$.*

Dans la suite de l'article, nous nous proposons de donner les principales étapes de la démonstration sans entrer dans tous les détails techniques.

3.– Réduction au cas d'un indice impair

Lemme 1.– *Soit $p \geq 5$ un nombre premier. Alors, tout diviseur premier de u_p est $\geq p$. De plus, si $p|u_p$ alors p divise Δ.*

Schéma de la démonstration : Si q est un diviseur premier de u_p alors q ne divise pas u_n pour $0 < n < p$. De plus, p divise $q + (\frac{\Delta}{q})$ (2), donc $q \geq p - 1$. Ainsi $q \geq p$, avec égalité seulement si $q|\Delta$. **CQFD**

Si p est un nombre premier et x un entier non nul, on désignera par $w_p(x)$ le plus grand entier k tel que p^k divise x.

Lemme 2.– *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 $u_{q^2} = \square$.*

Schéma de la démonstration : On remarque d'abord que u_q est impair et que $u_q|u_m$.

Soit r un diviseur premier de u_q. Soit $s = w_r(u_q)$ (3), alors $r^{s+1}|u_n$ si, et seulement si, $rq|n$. D'après le Lemme 1, $r \geq q$.

Si $r > q$, alors $w_r(u_m) = s$ et s est pair. Il s'ensuit que u_q est un carré si $q \not| \Delta$.

Reste le cas où $q|\Delta$ et où u_q n'est pas un carré. Alors $w_q(u_q)$ est impair et $w_q(u_{q^2}) = 1 + w_q(u_q)$ est pair. Les autres diviseurs de u_{q^2} sont $> q$ et l'argument précédent montre que u_{q^2} est un carré. **CQFD**

Lemme 3.– *Soient $a \geq 3$ et $m = 2^3 3^t$ 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 $m = 2^3 3^t$. 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 (ces deux formules sont immédiates en

(1) On notera qu'alors α et β, solutions de l'équation caractéristique, sont inverses l'un de l'autre.
(2) Le symbole $(\frac{x}{q})$ est le symbole de Legendre, caractère quadratique de x modulo q.
(3) Si r est un nombre premier et x un entier non nul on désigne par $w_r(x)$ l'entier h tel que $r^h|x$ et $r^{h+1} \not| x$.

utilisant les définitions de u et de v).

L'hypothèse de récurrence prouve qu'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 pour la paire (s, t) considérée.

Considérons d'abord le cas $m = 4$.

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 [L] 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 $a = \square$, $a^2 - 2 = 2\square$, soit $a = 4x^2$ et $16x^4 - 2 = 2y^2$: impossible modulo 8.

Si $u_4 = 3\square$ ou $6\square$ alors, comme $u_4 = a(a^2 - 2)$, on a $3|a$ 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

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

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 $v_3 = \square$, ces deux cas sont donc impossibles.

Si $a \equiv 1 \bmod 3$ alors 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 $a \equiv -1 \bmod 3$ alors ni 2 ni 3 ne divisent $a^3 - 3a - 1$. L'équation $a^3 - 3a - 1 = x^2$ impose $a \equiv 1 \bmod 4$. Si $a^3 - 3a + 1 = y^2$ alors $x^2 - y^2 = 2$, ce qui est impossible. Donc $a^3 - 3a + 1 = 3y^2$, et ainsi $(\frac{3}{a}) = 1$. Mais, puisque $a \equiv 1 \bmod 4$, on a $(\frac{3}{a}) = (\frac{a}{3}) = (\frac{-1}{3}) = -1$: contradiction.

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

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 4 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 $v_3 = a(a^2 - 3)$ et que $a^2 - 1 = 2\square$, $a^2 - 3 \neq 2\square$, on a $a = 3z^2, a^2 - 3 = 9z^4 - 3 = 3t^2, 9z^4 - 1 = 2x^2$. Modulo 5, ceci implique $z \not\equiv 0$ et donc $z^4 \equiv 1$, puis $6 \equiv 3t^2$, ce qui est impossible.

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

• $v_3 = \square$ implique $a = 1$. Dans ce cas $3|u_3$, ainsi $3 \not| a$ et donc $3 \not| v_3$. Donc $a = \square$ et $a^2 - 1 = \square$, ce qui impose $a = 1$.

• $u_3 = \square$ n'est possible que pour $a = 1$.

• $v_3 = 2\ \square$, $u_3 = 3\ \square$ ou $u_3 = 6\ \square$ ne peuvent avoir lieu que pour $a = 2$. En effet $3 \not| a$, et donc $a^2 - 3 = \square$ ou $2\ \square$. La première équation possède la solution unique $a = 2$, la seconde est impossible modulo 3.

• $u_3 = 2x^2$, $v_3 = 3\ \square$ ou $6\ \square$. 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 [L], 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 4.– *Le système d'équations en nombres entiers positifs*

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

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

Démonstration : La première équation implique $6Z^2 - (2Y)^2 = 2$. Or dans l'anneau $\mathbb{Z}[\sqrt{6}]$, 2 admet la décomposition : $2 = (5 - 2\sqrt{6})(2 + \sqrt{6})^2$ où $5 - 2\sqrt{6}$ est une unité (4) et $2 + \sqrt{6}$ est un élément premier. Or dans cet anneau toutes les unités sont de la forme $\pm(5 + 2\sqrt{6})^k$, $k \in \mathbb{Z}$. Par suite la première équation s'écrit aussi

$$(\sqrt{6}Z + 2Y)(\sqrt{6}Z - 2Y) = (2 + \sqrt{6})^2(5 + 2\sqrt{6})^{-1}$$

et donc il existe un entier $s \in \mathbb{Z}$ tel que

$$2Y + \sqrt{6}Z = (2 + \sqrt{6})(5 + 2\sqrt{6})^s$$

et par conjugaison $2Y - \sqrt{6}Z = (2 - \sqrt{6})(5 - 2\sqrt{6})^s$ ce qui conduit à

$$Z = \frac{(2 + \sqrt{6})(5 + 2\sqrt{6})^s - (2 - \sqrt{6})(5 - 2\sqrt{6})^s}{2\sqrt{6}}.$$

De la même façon avec la seconde relation, en se plaçant dans l'anneau $\mathbb{Z}[\sqrt{2}]$ où les unités sont de la forme $\pm(3 + 2\sqrt{2})^k$ on trouve:

$$3Z + \sqrt{2}X = (3 + 2\sqrt{2})^t$$
$$\text{et } 3Z - \sqrt{2}X = (3 - 2\sqrt{2})^t, t \in \mathbb{Z},$$

(4) dans un anneau une unité est un élément inversible.

ce qui conduit à : $Z = \frac{(3+2\sqrt{2})^t+(3-2\sqrt{2})^t}{6}$. L'égalisation des deux expressions permet d'écrire :

$$\frac{(3+\sqrt{6})(5+2\sqrt{6})^s}{(3+2\sqrt{2})^t} = \frac{1+(3-2\sqrt{2})^{2t}}{1+(5-2\sqrt{6})(5-2\sqrt{6})^{2s}}.$$

Il en résulte que la quantité

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

vérifie $|\Lambda| \leq 4(5+2\sqrt{6})^{-2s}$. Une application de l'estimation de M. Waldschmidt [W] fournit la borne $t \leq 10^{21}$. Ensuite, on procède comme et Davenport en [B-D] : 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 5.– (Baker-Davenport, [B-D]).– *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.– Principes de la démonstration du théorème

4.1. Etude de certaines unités

Les racines du polynôme $X^2 - aX + 1$ sont α et β. On considère le polynôme $X^4 + \Delta X^2 - \Delta$ dont les racines sont $\theta = i\sqrt{\alpha\sqrt{\Delta}}$, $-\theta$, $\theta_1 = \sqrt{\beta\sqrt{\Delta}}$ et $-\theta_1$.

Le corps $K = \mathbb{Q}(\theta)$ est un corps quartique où les conjugués de θ sont $-\theta, \theta_1$ et $-\theta_1$ et qui admet exactement deux plongements réels. D'après un théorème de Dirichlet (voir, par exemple, [P-K]), le rang du groupe des unités de K est donc égal à deux. On remarque que α et $\varepsilon = 1 + \theta$ sont des unités de K (c'est-à-dire des unités de l'anneau des entiers de K).

On peut montrer que $\{\alpha, \varepsilon\}$ est un système fondamental d'unités de l'anneau $\mathbb{Z}[\theta]$.

4.2. Utilisation de la théorie de Baker

Supposons que le nombre $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ soit le carré d'un entier x, alors $\alpha^{n+1} = \alpha\sqrt{\Delta}x^2 + \alpha\beta^n$. Lorsque n est impair, $n = 2m + 1$, 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 tels que

$$\theta x + \beta^m = \beta^u\varepsilon^v,\ -\theta x + \beta^m = \beta^u\varepsilon^{-v}\ , \theta_1 x + \alpha^m = \alpha^u\varepsilon_1^v \text{ et } -\theta_1 x + \alpha^m = \alpha^u\varepsilon_1'^v.$$

En eliminant x entre ces relations, il vient

$$\theta_1\beta^u(\varepsilon^v - \varepsilon^{-v}) = \theta\alpha^u(\varepsilon_1^v - \varepsilon_1'^v).$$

D'où l'on tire facilement

$$u \approx \frac{v-1}{2}\Big(1-\frac{\log 2}{\log a}\Big) \quad \text{et} \quad m \approx \frac{v-1}{2}\Big(1+\frac{\log 2}{\log a}\Big).$$

Il existe un entier k tel que

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

vérifie $|\Lambda| \leq 4\beta^{2m}$. Par ailleurs, en utilisant les résultats de [M-W], on peut minorer la "forme linéaire" $|\Lambda|$ par

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

Il en résulte que $v \leq V = 1.1 \times 10^6$. En développant $\log(\varepsilon/\bar{\varepsilon})$, on obtient

$$\Lambda = i\pi\Big(v - \frac{2v}{\pi}(\frac{1}{\theta}+\frac{1}{3\theta^2}+\cdots) - k\Big).$$

On voit que pour $v = k$ on a $|\Lambda| \geq 1/(2a)$, ce qui contredit la majoration précédente de Λ; on a donc $v \neq k$, ce qui implique $|v| \geq \pi(a-4)/2$. Par ailleurs, $|v| \geq 1.9m$ pour $a \geq 700000$. Donc $a \leq 800000$.

Un calcul sur ordinateur montre que $|\Lambda| \geq 3a^{-3}v^{-2}$ pour $16 < a \leq 800000$ et $0 < v \leq V$. Pour ces valeurs de a, il s'ensuit que l'on a $v \leq 5$. D'où $a \leq 7$: contradiction.

Pour $4 \leq a \leq 16$, on a $|\Lambda| \geq 1/(2700v^2)$ si $0 < v \leq V$. D'où $v \leq 15$, puis $m \leq 9$, et une vérification directe montre qu'il n'y a pas de solution.

Le théorème est alors une conséquence directe des lemmes 2 et 3. (On peut remarquer que $u_3 = a^2 - 1$ n'est jamais un carré.)

Références

[B-D] A. BAKER et H. DAVENPORT.– The equations $3x^2-2=y^2$ et $8x^2-7=z^2$; *Quart. J. Math. Oxford*, **2**, 1969, p. 129-137.

[C] J.H.E. COHN.– On square Fibonacci numbers; *J. London Math. Soc.*, **39**, 1957, p. 537-540.

[L] W. LJUNGREEN.– Zur Theorie der Gleichung $x^2+1=Dy^4$; *Avh. Norske Vid. Akad. Oslo*, No. 5, **1**, 1942.

[McD-R] W.L. McDANIEL et P. RIBENBOIM.– Squares and double-squares in Lucas sequences; *C.R. Math. Rep. Acad. Sci. Canada*, Vol. 14, n° 2, 3, 1992, p. 104-108.

[M-P] M. MIGNOTTE et A. PETHÖ.– Sur les carrés dans certaines suites de Lucas; manuscrit, Strasbourg, sept. 1992.

[M-W] M. MIGNOTTE et M. WALDSCHMIDT.– Linear forms in two logarithms and Schneider's method, III; *Annales Fac. Sci. Toulouse*, 1990, p. 43-75.

[P-Z] M. POHST & H. ZASSENHAUS.– *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[W] M. WALDSCHMIDT.– Minorations de combinaisons linéaires de logarithmes de nombres algébriques; *Canadian J. Math.*, à paraître.