Journal de Théorie des Nombres
de Bordeaux **18** (2006), 299–313

Les nombres de Lucas et Lehmer sans diviseur primitif

par Mourad ABOUZAID

Résumé. Y. Bilu, G. Hanrot et P.M. Voutier ont montré que pour toute paire de Lucas ou de Lehmer (α, β) et pour tout $n > 30$, les nombres entiers, dits de Lucas (ou de Lehmer) $u_n(\alpha, \beta)$ admettaient un diviseur primitif. L'objet de ce papier est de compléter la liste des nombres de Lucas et de Lehmer défectueux donnée par P.M. Voutier, afin d'en avoir une liste exhaustive.

Abstract. Y. Bilu, G. Hanrot et P.M. Voutier showed that for any Lucas or Lehmer's pair (α, β) and for all $n > 30$, rational integers $u_n(\alpha, \beta)$, said Lucas or Lehmer numbers had a primitive divisor. The purpose of this paper is to complete the list of defective Lucas or Lehmer's numbers given by P.M. Voutier, so that we have an exhaustive list.

1. Introduction

A la fin du XIX$^{\text{ième}}$ siècle, Lucas [5], [6] propose une étude poussée des nombres dits *de Lucas* définis comme suit : une *paire de Lucas* est une paire (α, β) d'entiers algébriques racines d'un polynôme de degré deux à discriminant positif, tels que $\alpha + \beta$ et $\alpha\beta$ soient dans $\mathbb{Z} - \{0\}$, premiers entre eux et tels que α/β ne soit pas une racine de l'unité. A toute paire de Lucas (α, β) on associe une suite d'entiers $(u_n)_{n\in\mathbb{N}^*}$ dite de *nombres de Lucas*, définie par :

$$\forall n \in \mathbb{N}^*, \;\; u_n = u_n(\alpha, \beta) = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

Lucas en donne de nombreuses propriétés arithmétiques, ainsi que d'importantes applications telles que l'approximation rapides d'entiers quadratiques ou des tests de primalité pour les nombres de Mersenne.

En 1913, Carmichael se penche sur les travaux de Lucas en s'intéressant en particulier aux diviseurs primitifs des nombres de Lucas ([2]). Etant donnée une paire de Lucas (α, β) et un entier n, un diviseur premier de u_n sera dit *primitif* s'il ne divise pas le produit $(\alpha - \beta)^2 u_1 ... u_{n-1}$. En notant

Manuscrit reçu le 5 octobre 2004.

P l'application qui à un entier associe sont plus grand diviseur premier, Carmichael montre également que pour $n > 12$, on a

$$P(u_n) \geqslant n - 1.$$

Il en déduit que pour n assez grand, tout nombre u_n admet un diviseur primitif.

En 1930 dans [4], Lehmer généralise les résultats de Lucas en définissant ses propres suites : une *paire de Lehmer* est une paire (α, β) d'entiers algébriques, racines d'un polynôme de degré deux à discriminant strictement positif, tels que $(\alpha+\beta)^2$ et $\alpha\beta$ soient dans $\mathbb{Z}-\{0\}$, premiers entre eux et tels que α/β ne soit pas une racine de l'unité. A toute paire de Lehmer (α, β) on associe une suite d'entiers $(\tilde{u}_n)_{n\in\mathbb{N}^*}$ dite de *nombres de Lehmer* définie par :

$$\forall n \in \mathbb{N}^*,\ \ \tilde{u}_n = \tilde{u}_n(\alpha,\beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta) & \text{si } n \text{ est impair,} \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{si } n \text{ est pair.} \end{cases}$$

Un diviseur premier de $\tilde{u}_n$ sera dit primitif s'il ne divise pas le produit $(\alpha^2 - \beta^2)^2\tilde{u}_1 \dots \tilde{u}_{n-1}$.

En 1955, Ward [10] se penche a son tour sur les nombres de Lehmer, et comme Carmichael l'avait fait pour les nombres de Lucas, il montre que pour $n > 18$, tout nombre $\tilde{u}_n$ admet un diviseur primitif. Ce résultat sera amélioré pas Dust qui montre en 1965 dans [3] qu'il suffit de prendre $n > 12$.

En 1962, Schinzel [7] étend la définition des nombres de Lucas et Lehmer au cas des polynômes de degré deux à discriminant négatifs et montre là encore que pour tout couple (α, β) et pour tout n assez grand, u_n et $\tilde{u}_n$ admettent un diviseur primitif. Y. Bilu, G. Hanrot et P.M. Voutier [1] ont montré que c'etait le cas dés que $n > 30$. P. M. Voutier donne également dans [9] une liste exhaustive des paires de Lucas n-défectueuses pour $4 < n \leqslant 30,\ \ n \neq 6$ et des paires de Lehmer n-défectueuses pour $6 < n \leqslant 30,\ \ n \notin \{8, 10, 12\}$. (On dira qu'une paire (α, β) est n-défectueuse si le $n^{\text{ième}}$ terme de la suite associée à (α, β) ne possède pas de diviseur primitif.).

L'objet de ce papier est de reprendre en détails les démonstrations faites dans [1] afin de combler les trous laissés par Voutier et de donner une liste complète des paires de Lucas et Lehmer défectueuses. Les corrections apportées à [1] seront notées en gras, sauf dans le cas $n = 12$ où l'approche est un peu différente.

Remarque : toute paire de Lucas (α, β) est également une paire de Lehmer et :

$$u_n = \begin{cases} \tilde{u}_n & \text{si } n \text{ est impair,} \\ (\alpha + \beta)\tilde{u}_n & \text{si } n \text{ est pair.} \end{cases}$$

Ainsi, si (α, β) est une paire de Lucas et $n \in \mathbb{N}\backslash\{2\}$, tout nombre premier r est un diviseur primitif de u_n si et seulement si c'est un diviseur primitif

de $\tilde{u}_n$ et une paire de Lucas (α, β) est n-défectueuse si et seulement si c'est une paire de Lehmer n-défectueuse.

Au vu de la forme des termes $u_n(\alpha, \beta)$ et $\tilde{u}_n(\alpha, \beta)$, il est naturel de considérer les polynômes cyclotomiques

$$\Phi_n(X, Y) = \prod_{\substack{1 \leqslant k < n \\ (k,n)=1}} (X - e^{2ik\pi/n} Y)$$

et leurs valeurs en (α, β). Ainsi, pour tout $n \in \mathbb{N}^*$ on a :

$$\alpha^n - \beta^n = \prod_{d|n} \Phi_d(\alpha, \beta), \tag{1.1}$$

$$u_n = \prod_{d|n,\ d \neq 1} \Phi_d(\alpha, \beta), \quad \tilde{u}_n = \prod_{d|n,\ d>2} \Phi_d(\alpha, \beta). \tag{1.2}$$

En particulier, pour tout $n \in \mathbb{N}^*$, $\Phi_n(\alpha, \beta)$ divise u_n et $\tilde{u}_n$.

Cela nous permettra, après une étude rapide de l'arithmétique des suites de Lucas et de Lehmer, d'énoncer un *critère cyclotomique* donnant des restrictions importantes et décisives concernant les paires de Lucas et Lehmer. La deuxième partie sera consacrée à l'étude exhaustive des cas laissés de coté par Voutier.

2. Critère cyclotomique

2.1. Quelques lemmes préliminaires.

Proposition 2.1. *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m \in \mathbb{N}^*}$ la suite de Lehmer correspondante. Alors :*

(1) *Pour tout $m > 0$, on a $(\alpha\beta, \tilde{u}_m) = 1$.*

(2) *Si d divise m, alors $\tilde{u}_d$ divise $\tilde{u}_m$ et $(\tilde{u}_m/\tilde{u}_d, \tilde{u}_d)$ divise m/d.*

(3) *Pour tous entiers positifs m et n on a $(\tilde{u}_m, \tilde{u}_n) = \tilde{u}_{(m,n)}$.*

(4) *Si un nombre premier r ne divise pas $\alpha\beta(\alpha^2 - \beta^2)^2$ alors r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}$.*

(5) *Si un nombre premier r divise $\tilde{u}_m$ alors r divise $\tilde{u}_{mr}/\tilde{u}_m$. De plus, si $r > 2$, alors r divise exactement $\tilde{u}_{mr}/\tilde{u}_m$ (i.e. r^2 ne divise pas $\tilde{u}_{mr}/\tilde{u}_m$).*

(6) *Si 4 divise $\tilde{u}_m$, alors 2 divise exactement $\tilde{u}_{2m}/\tilde{u}_m$.*

(7) *Si un nombre premier $r > 2$ divise $(\alpha - \beta)^2$, alors r divise $\tilde{u}_r$.*
De plus, si $r > 3$, alors r divise exactement $\tilde{u}_r$.

(8) *Si un nombre premier r divise $(\alpha + \beta)^2$, alors r divise $\tilde{u}_{2r}$.*
De plus, si $r > 3$, alors r divise exactement $\tilde{u}_{2r}$.

Démonstration. Pour cette preuve, on notera $N_1, N_2, \ldots, N_7$ des entiers algébriques dépendant de α, β et des indices des termes des suites (u_n), (v_n) et $(\tilde{u}_n)$ que l'on considère. Soit donc (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. On définit une nouvelle suite $(v_m)_{m\in\mathbb{N}^*}$:

$$\forall m \in \mathbb{N}^*, \ \ v_m = \begin{cases} (\alpha^m + \beta^m)/(\alpha+\beta) & \text{si } m \text{ est impair,} \\ \alpha^m + \beta^m & \text{si } m \text{ est pair.} \end{cases}$$

1 : Pour tout $m \in \mathbb{N}^*$ on a :

$$\begin{aligned}(\alpha+\beta)^{2m} &= \alpha^{2m} + \beta^{2m} + \alpha\beta N_0 = v_{2m} + \alpha\beta N_0 \\ &= (\alpha^{2m+1} + \beta^{2m+1})/(\alpha+\beta) + \alpha\beta N_1 = v_{2m+1} + \alpha\beta N_1\end{aligned}$$

où les N_i sont des nombres algebriques. Or par hypothèse, $\alpha\beta$ et $(\alpha+\beta)^2$ sont premiers entre eux donc $\alpha\beta$ et v_m le sont également. De même pour tout m impair,

$$\tilde{u}_m = (\alpha^m - \beta^m)/(\alpha-\beta) = v_{m-1} + \alpha\beta N_2$$

et pour m pair,

$$\tilde{u}_m = (\alpha^m - \beta^m)/((\alpha-\beta)(\alpha+\beta)) = v_{m-1} + \alpha\beta N_3.$$

Donc pour tout m, $(\alpha\beta, v_m) = 1$ impose $(\alpha\beta, \tilde{u}_m) = 1$.

2 : Soient $m \in \mathbb{N}$ et d un diviseur de m. D'après (1.2) il est clair que $\tilde{u}_d$ divise $\tilde{u}_m$. D'autre part, comme $\alpha^m = (\beta^d + (\alpha^d - \beta^d))^{m/d}$ on a :

$$\frac{\alpha^m - \beta^m}{\alpha^d - \beta^d} = \sum_{k=1}^{m/d} \begin{pmatrix} m/d \\ k \end{pmatrix} (\alpha^d - \beta^d)^{k-1} \beta^{m-kd}.$$

En multipliant de chaque coté par α^{m-d} il vient :

$$\alpha^{m-d}\frac{\tilde{u}_m}{\tilde{u}_d} = \frac{m}{d}(\alpha\beta)^{m-d} + N_4\tilde{u}_d \text{ si } m-d \text{ est pair,} \tag{2.1}$$

$$\alpha^{m-d}(\alpha+\beta)\frac{\tilde{u}_m}{\tilde{u}_d} = \frac{m}{d}(\alpha\beta)^{m-d} + N_5\tilde{u}_d \text{ si } m-d \text{ est impair.} \tag{2.2}$$

Comme $(\alpha\beta, \tilde{u}_d) = 1$, l'assertion *2* est démontrée.

3 : Soient m et n deux entiers positifs. Il existe s et t dans $\mathbb{N}$ tels que $tm - sn = (m,n) = d$ $(*)$. Notons alors $m = dm'$, $n = dn'$, $k = tm$ et $l = sn$. D'après $(*)$, $tm' - sn' = 1$ donc t et s, t et n', s et m' sont respectivement premiers entre eux. Ainsi $(k,l) = d$ et $k - l = (k,l)$.

D'autre part $(\alpha^k - \beta^k)(\alpha^l + \beta^l) - (\alpha^k + \beta^k)(\alpha^l - \beta^l) = 2(\alpha\beta)^l(\alpha^{k-l} - \beta^{k-l})$ donc

$$\tilde{u}_k v_l - \tilde{u}_l v_k = 2(\alpha\beta)^l \tilde{u}_{k-l} \text{ si } k-l \text{ est pair,} \tag{2.3}$$

$$(\alpha+\beta)^2\tilde{u}_k v_l - \tilde{u}_l v_k = 2(\alpha\beta)^l \tilde{u}_{k-l} \text{ si } k-l \text{ et } l \text{ sont impairs,} \tag{2.4}$$

(2.5) $\qquad \tilde{u}_k v_l - (\alpha+\beta)^2 \tilde{u}_l v_k = 2(\alpha\beta)^l \tilde{u}_{k-l}$ si $k-l$ et k sont impairs.

Si 2 ne divise pas $(\tilde{u}_k, \tilde{u}_l)$, d'après l'assertion *1*, $(\tilde{u}_k, \tilde{u}_l)$ divise $\tilde{u}_{k-l}$. Supposons donc que 2 divise $(\tilde{u}_k, \tilde{u}_l)$. Comme $\tilde{u}_{2k}/\tilde{u}_k = v_k$, d'après (2.1) et (2.2), comme $\alpha\beta$ et v_k sont premiers entre eux, 2 divise v_k si k est pair et $(\alpha+\beta)^2$ si k est impair. Il en va de même pour l donc dans tous les cas, comme $\alpha\beta$ est premier avec tous les $\tilde{u}_m$, $(\tilde{u}_k, \tilde{u}_l)$ divise $\tilde{u}_{k-l}$. Par ailleurs, comme $k-l$ divise k et l, $\tilde{u}_{k-l}$ divise $(\tilde{u}_k, \tilde{u}_l)$, d'où l'égalité.

4 : Soit r un nombre premier ne divisant pas $\alpha\beta(\alpha^2-\beta^2)^2$. Si $r>2$, on a

$$\begin{aligned}(\alpha^2-\beta^2)^2 \tilde{u}_{r-1}\tilde{u}_{r+1} &= (\alpha^{r-1}-\beta^{r-1})(\alpha^{r+1}-\beta^{r+1}) \\ &= \alpha^{2r}+\beta^{2r}-(\alpha\beta)^{r-1}(\alpha^2+\beta^2).\end{aligned}$$

Or comme r ne divise pas $\alpha\beta$, d'après le petit théorème de Fermat, il vient :

$$(\alpha-\beta)^2(\alpha+\beta)^2 \tilde{u}_{r-1}\tilde{u}_{r+1} \equiv 0 \bmod r,$$

Et comme r est premier avec $(\alpha-\beta)^2(\alpha+\beta)^2$, r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}$.

Pour $r=2$, on a :

$$\tilde{u}_{r-1}\tilde{u}_{r+1} = \tilde{u}_3 = \alpha^2+\alpha\beta+\beta^2 = (\alpha+\beta)^2-\alpha\beta.$$

Donc si 2 ne divise ni $\tilde{u}_3$ ni $\alpha\beta$, alors 2 divise $(\alpha+\beta)^2$, ce qui prouve l'assertion *4*.

5 : Soient $m \in \mathbb{N}^*$ et r un nombre premier. Comme dans la preuve du *2*, on a :

$$(2.6) \quad \frac{\alpha^{rm}-\beta^{rm}}{\alpha^m-\beta^m} = \sum_{k=1}^{r-1} \begin{pmatrix} r \\ k \end{pmatrix} (\alpha^m-\beta^m)^{k-1}\beta^{m(r-k)} + (\alpha^m-\beta^m)^{r-1}.$$

Or pour tout $k \in \{1, ..., r-1\}$, r divise $\begin{pmatrix} r \\ k \end{pmatrix}$. De plus, $\alpha^m-\beta^m = N_6\tilde{u}_m$. Donc si r divise $\tilde{u}_m$ alors r divise $(\alpha^{rm}-\beta^{rm})/(\alpha^m-\beta^m) = \tilde{u}_{rm}/\tilde{u}_m$.

D'autre part, si $r>2$, de (2.6) on tire également

$$(2.7) \quad \alpha^{m(r-1)}\frac{\tilde{u}_{rm}}{\tilde{u}_m} - r(\alpha^m-\beta^m)N_7 - (\alpha^m-\beta^m)^{r-1}\alpha^{m(r-1)} = r(\alpha\beta)^{m(r-1)}.$$

Donc si r divise $\tilde{u}_m$ alors r divise $\alpha^m-\beta^m$ et comme $(\alpha\beta, \tilde{u}_m)=1$, r^2 ne peut diviser $\tilde{u}_{rm}/\tilde{u}_m$.

6 : soit $m \in \mathbb{N}^*$ tel que 4 divise $\tilde{u}_m$. Alors,

$$\frac{\alpha^{2m}-\beta^{2m}}{\alpha^m-\beta^m} = 2\beta^m + (\alpha^m-\beta^m).$$

Or si m est pair, $(\alpha^{2m}-\beta^{2m})/(\alpha^m-\beta^m) = \tilde{u}_{2m}/\tilde{u}_m$. Donc si 4 divise $\tilde{u}_m$ alors 4 divise $(\alpha^m-\beta^m)$ mais 4 ne divise pas $2\beta^m$ car $(\alpha\beta, \tilde{u}_m)=1$. Donc 2 divise exactement $\tilde{u}_{2m}/\tilde{u}_m$.

Par ailleurs, si m est impair, $(\alpha^{2m}-\beta^{2m})/(\alpha^m-\beta^m) = (\alpha+\beta)\tilde{u}_{2m}/\tilde{u}_m$. Si 2 ne divise pas $(\alpha+\beta)^2$, 2 divise donc exactement $\tilde{u}_{2m}/\tilde{u}_m$. Enfin, si 2 divise $(\alpha+\beta)^2$, alors 2 divise $\tilde{u}_4 = (\alpha+\beta)^2 - 2\alpha\beta$ et d'après l'assertion *3*, $(\tilde{u}_4, \tilde{u}_m) = 1$ donc 2 ne peut pas diviser $\tilde{u}_m$.

7 : soit $r > 2$ un nombre premier. En posant $m = 1$ dans l'équation (2.6) il vient :

$$\tilde{u}_r = \frac{\alpha^r - \beta^r}{\alpha - \beta} = \sum_{k=1}^{r-1} \left(\begin{array}{c} r \\ k \end{array} \right) (\alpha-\beta)^{k-1}\beta^{(r-k)} + (\alpha-\beta)^{r-1}.$$

Donc si r divise $(\alpha-\beta)^2$ alors r divise $\tilde{u}_r$. De plus, si $r > 3$, r^2 divise tous les termes du second membre de l'équation précédente sauf pour $k = 1$. Donc r^2 ne peut diviser $\tilde{u}_r$.

8 : le raisonnement est le même que pour le cas précédent en posant ici $m = 2$. □

Corollaire 2.1. *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Pour tout nombre premier r qui ne divise pas $\alpha\beta$ il existe un entier positif m tel que r divise $\tilde{u}_m$.*

Démonstration. Soit r un nombre premier qui ne divise pas $\alpha\beta$. Alors d'après les assertions *4*, *7* et *8*, r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}\tilde{u}_r\tilde{u}_{2r}$. Il existe donc $m > 0$ tel que r divise $\tilde{u}_m$. □

Notons m_r le plus petit entier positif ayant cette propriété.

Corollaire 2.2. *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Alors pour tout entier r ne divisant pas $\alpha\beta$, on a*

$$r|\tilde{u}_m \Leftrightarrow m_r|m. \tag{2.8}$$

Démonstration. ($\Leftarrow$) : d'après l'assertion *2*, si m_r divise m alors $\tilde{u}_{m_r}$ divise $\tilde{u}_m$. Or par définition, r divise $\tilde{u}_{m_r}$ donc r divise $\tilde{u}_m$.

($\Rightarrow$) : d'après l'assertion *3*, si r divise $\tilde{u}_m$ alors r divise $(\tilde{u}_{m_r}, \tilde{u}_m) = \tilde{u}_{(m_r,m)}$. Or m_r étant minimal, $m_r \leqslant (m_r, m)$, ce qui n'est possible que si m_r divise m. □

Corollaire 2.3. *Soit (α, β) une paire de Lehmer et $(\tilde{u}_m)_{m\in\mathbb{N}^*}$ la suite de Lehmer correspondante. Alors pour tout entier r ne divisant pas $\alpha\beta$, on a*

$$m_r = r \text{ si } r > 2 \text{ et } r|(\alpha-\beta)^2, \tag{2.9}$$

$$m_r = 2r \text{ si } r|(\alpha+\beta)^2, \tag{2.10}$$

$$m_r|(r-1) \text{ ou } m_r|(r+1) \text{ sinon.} \tag{2.11}$$

Démonstration. Formule (2.9) : si $r > 2$ et r divise $(\alpha-\beta)^2$ alors d'après l'assertion *7*, r divise $\tilde{u}_r$. De plus, d'après (2.8), m_r divise r donc $m_r = r$.

Formule (2.11) : pour $r > 2$, si l'on est pas dans les cas (2.9) ou (2.10), d'après l'assertion *4*, r divise $\tilde{u}_{r-1}\tilde{u}_{r+1}$. D'après (2.8), m_r divise donc $(r-1)$ ou $(r+1)$. D'autre part, pour $r = 2$, si 2 ne divise pas $(\alpha+\beta)^2$, alors 2 ne divise pas non plus $(\alpha-\beta)^2$ et toujours d'après l'assertion *4*, 2 divise $\tilde{u}_1\tilde{u}_3$.

Formule (2.10) : si r divise $(\alpha+\beta)^2$, d'après l'assertion *8*, r divise $\tilde{u}_{2r}$. Ainsi, d'après (2.8), on a $m_r = r$ ou $m_r = 2r$. Montrons qu'alors r ne peut pas diviser $\tilde{u}_r$. Si $r = 2$, alors $\tilde{u}_2 = 1$ et il n'y a rien à faire. Si $r > 2$, on a

$$\alpha^r - \beta^r \equiv (\alpha-\beta)^r \bmod r. \tag{2.12}$$

Or $(\alpha+\beta)^2$ et $\alpha\beta$ étant premiers entre eux, $((\alpha+\beta)^2, (\alpha-\beta)^2)$ divise 4 donc si r divise $(\alpha+\beta)^2$, il est premier avec $(\alpha-\beta)$. En divisant l'équation (2.12) il vient

$$\tilde{u}_r \equiv (\alpha-\beta)^{r-1} \not\equiv 0 \bmod r.$$

Donc r ne divise pas $\tilde{u}_r$ et $m_r = 2r$. □

En particulier, si 2 ne divise pas $\alpha\beta$ alors

$$m_2 = \begin{cases} 4 & \text{si } 2|(\alpha^2-\beta^2)^2, \\ 3 & \text{sinon.} \end{cases} \tag{2.13}$$

et si 3 ne divise pas $\alpha\beta$ alors

$$m_3 = \begin{cases} 3 \text{ ou } 6 & \text{si } 3|(\alpha^2-\beta^2)^2, \\ 4 & \text{sinon.} \end{cases} \tag{2.14}$$

Proposition 2.2. *Soit (α,β) une paire de Lehmer et soit r un diviseur premier de $\Phi_n(\alpha,\beta)$, $n > 2$. Alors r ne divise pas $\alpha\beta$ et il existe $k \geqslant 0$ tel que $n = m_r r^k$.*

Démonstration. Soient $n > 2$ et r un diviseur premier de $\Phi_n = \Phi_n(\alpha,\beta)$. Comme Φ_n divise $\tilde{u}_n$, d'après l'assertion *1* de la proposition 2.1, r ne divise pas $\alpha\beta$. D'après le corollaire 2.2, m_r divise n. Il existe donc $t > 0$ et $k \geqslant 0$ tels que $(t,r) = 1$ et $n = m_r t r^k$. Supposons alors que $t > 1$. Toujours d'après le corollaire 2.2, r divise $\tilde{u}_{n/t}$. De plus, comme $n/t < n$, l'entier Φ_n divise encore $\tilde{u}_n/\tilde{u}_{n/t}$ et donc r divise également $\tilde{u}_n/\tilde{u}_{n/t}$. D'après l'assertion *2* de la propostion 2.1, il vient alors que r divise $\frac{n}{n/t} = t$, ce qui est exclu. Donc $t = 1$ et $n = m_r r^k$. □

2.2. Le critère cyclotomique. Rappelons que pour un entier n fixés, une paire de Lehmer (α,β) sera dite n-défectueuse si le $n^{\text{ième}}$ terme de la suite de Lehmer associée à (α,β) n'admet pas de diviseur primitif. D'autre part, pour n dans $\mathbb{N}^*$ notons $P(n)$ le plus grand diviseur premier de n et $P'(n) = P(n/(n,3))$. On peut alors énoncer le théorème suivant.

Théorème 2.1. (Critère cyclotomique) *Soit $n > 4$ un entier distinct de 6 et 12. Une paire de Lehmer (α, β) est n-défectueuse si et seulement si $\Phi_n(\alpha, \beta) \in \{\pm 1, \pm P'(n)\}$. De plus, une paire de Lehmer (α, β) est 12-défectueuse si et seulement si $\Phi_{12}(\alpha, \beta) \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$.*

Démonstration. ($\Rightarrow$) : soit $n \in \mathbb{N}^*$ tel que $n > 4$ et $n \neq 6$ et soit (α, β) une paire de Lehmer n-défectueuse. Soit r un diviseur premier de Φ_n. On a donc $r|\tilde{u}_n$ et d'après la proposition précédente, r ne divise pas $\alpha\beta$ et il existe $k \geqslant 0$ tel que $n = m_r r^k$. Comme $\tilde{u}_n$ n'admet pas de diviseur primitif, par minimalité de m_r il vient :

$$n = m_r r^k \text{ avec } k \geqslant 1, \tag{2.15}$$

ou

$$n = m_r \text{ et } r|(\alpha^2 - \beta^2)^2. \tag{2.16}$$

D'après le corollaire 2.3, on a donc :

$$r = \begin{cases} P'(n) & \text{si } n \neq 12, \\ 2 \text{ ou } 3 & \text{si } n = 12. \end{cases} \tag{2.17}$$

Il nous reste à montrer que r divise exactement Φ_n. Pour cela, on distingue les cas (2.15) et (2.16) :

• $n = m_r r^k$, $k \geqslant 1$: tout d'abord, comme m_r divise (n/r), d'après le corollaire 2.2, r divise $\tilde{u}_{n/r}$. On distingue alors les cas $r > 2$ et $r = 2$:

- Si $r > 2$, d'après l'assertion *5* de la proposition 2.1, il vient que r divise exactement $\tilde{u}_n/\tilde{u}_{n/r}$. Comme Φ_n divise également $\tilde{u}_n/\tilde{u}_{n/r}$, r divise exactement Φ_n.
- Si $r = 2$ et 2 ne divise pas $(\alpha^2 - \beta^2)^2$, d'après le corollaire 2.3, on a $m_2 = 3$ et donc $n = 3.2^k$, $k \geqslant 2$ (car $n \neq 6$). Par ailleurs, $\Phi_3 = \tilde{u}_3 = \alpha^2 + \beta^2 - \alpha\beta$. Donc comme 2 ne divise ni $\alpha\beta$ ni $\alpha^2 + \beta^2$, Φ_3 est pair. De plus, $\Phi_3 - \Phi_6 = 2\alpha\beta \equiv 2 \bmod 4$. Donc 4 divise Φ_3 ou Φ_6 et donc 4 divise $\tilde{u}_3$ ou $\tilde{u}_6$. Dans tous les cas, 4 divise $\tilde{u}_6$ (car $3|6 \Rightarrow \tilde{u}_3|\tilde{u}_6$ d'après l'assertion *2* de la proposition 2.1). Enfin, toujours d'après l'assertion *2* de la proposition 2.1, comme 6 divise $n/2$, 4 divise également $\tilde{u}_{n/2}$ et d'après la proposition 2.1, *6*, 2 divise exactement $\tilde{u}_n/\tilde{u}_{n/2}$. Il en est donc de même pour Φ_n.
- Enfin, si $r = 2$ et $2|(\alpha^2 - \beta^2)^2$, d'après le corollaire 2.3, $m_2 = 4$ et donc $n = 2^k$, $k \geqslant 3$. On démontre par récurrence sur k que pour tout $k \geqslant 3$, 2 divise exactement Φ_{2^k}. En effet, comme 2 divise $(\alpha - \beta)^2(\alpha + \beta)^2$, 2 divise l'un des deux facteurs et donc 2 divise $(\alpha^2 + \beta^2) = (\alpha - \beta)^2 + 2\alpha\beta = (\alpha + \beta)^2 - 2\alpha\beta$. Ainsi, 4 divise $(\alpha^2 + \beta^2)^2 = \alpha^4 + \beta^4 + 2(\alpha\beta)^2$. Donc comme $\alpha\beta \equiv 2 \bmod 4$, 2 divise exactement $\Phi_8 = \alpha^4 + \beta^4$. On montre de même que si 2 divise $(\alpha^{2^{k-1}} + \beta^{2^{k-1}} = \Phi_{2^k}$ alors 2 divise exactement $\alpha^{2^k} + \beta^{2^k} = \Phi_{2^{k+1}}$.

• $n = m_r$ et $r|(\alpha^2 - \beta^2)^2$: comme $n \notin \{3, 4, 6\}$, alors $r > 3$. D'après les assertions *7* et *8* de la proposition 2.1, r divise donc exactement $\tilde{u}_n = \tilde{u}_{m_r}$, ce qui termine la première partie de la démonstration.

Implication ($\Leftarrow$) : soit $n \in \mathbb{N}^*$ tel que $n > 4$ et $n \neq 6$ et soit (α, β) une paire de Lehmer telle que

$$\Phi_n \in \begin{cases} \{\pm 1, \pm P'(n)\} & \text{si } n \neq 12, \\ \{\pm 1, \pm 2, \pm 3, \pm 6\} & \text{si } n = 12. \end{cases} \tag{2.18}$$

Montrons qu'alors, (α, β) est n-défectueuse.

Soit r un diviseur premier de $\tilde{u}_n$. D'après (1.2), $\tilde{u}_n$ apparait comme étant un élement du groupe multiplicatif engendré par les $\{\Phi_m,\ m > 2,\ m|n\}$, $(\alpha+\beta)^2$ et $(\alpha-\beta)^2$. Donc r divise l'un de ces nombres. Mais alors r divise $(\alpha^2-\beta^2)^2 \prod_{1 \leqslant k < n} \tilde{u}_k$ et ça n'est pas un diviseur primitif de $\tilde{u}_n$. Et si r divise Φ_n alors d'après (2.18), r vérifie (2.17). En particulier, $r|n$. Si $m_r < n$ alors par définition de m_r, r n'est pas un diviseur primitif de $\tilde{u}_n$ et si $m_r = n$, d'après le corollaire 2.3, r divise $(\alpha^2 - \beta^2)^2$ ce qui prouve encore que r n'est pas un diviseur primitif de $\tilde{u}_n$ et qui termine la démonstration du théorème 2.1. □

3. Les paires de Lucas et Lehmer défectueuses

Dans la suite, les paires de Lehmer (α, β) défectueuses seront données par un couple (a, b) tel que $\alpha, \beta = \frac{\sqrt{a} \pm \sqrt{b}}{2}$. Par ailleurs, on notera $p = (\alpha + \beta)^2$ et $q = \alpha\beta \neq 0$. Ainsi, $a = p$ et $b = p - 4q$. De même, les paires de Lucas (α, β) défectueuses seront données par un couple (a, b) tel que $\alpha, \beta = \frac{a \pm \sqrt{b}}{2}$. Par ailleurs, on notera $m = \alpha + \beta = \sqrt{p}$ et $q = \alpha\beta \neq 0$. Ainsi, $a = m$ et $b = m^2 - 4q$.

3.1. Restrictions. Deux paires de Lucas (α_1, β_2) et (α_2, β_2) seront dites *équivalentes* si $\alpha_1/\alpha_2 = \beta_1/\beta_2 = \pm 1$. Deux paires de Lehmer (α_1, β_2) et (α_2, β_2) seront dites *équivalentes* si $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm i\}$. Si (α_1, β_2) et (α_2, β_2) sont deux paires de Lucas (resp. Lehmer) équivalentes, $u_n(\alpha_1, \beta_1) = \pm u_n(\alpha_2, \beta_2)$ (resp. $\tilde{u}_n(\alpha_1, \beta_1) = \pm \tilde{u}_n(\alpha_2, \beta_2)$). Ainsi, si une paire est n-défectueuse pour un n donné, il en est de même pour toute paire équivalente, et l'on pourra parfois choisir le signe de u_n (resp. $\tilde{u}_n$).

D'autre part, α/β n'étant pas une racine de l'unité, on a nécessairement

$$(p, q) \notin \{\pm(1, 1), \pm(2, 1), \pm(3, 1), \pm(4, 1)\}. \tag{3.1}$$

En effet, si l'on note $\gamma = \alpha/\beta$, comme α et β sont les racines du polynôme $X^2 - \sqrt{p}X + q$, on vérifie rapidement que γ et γ^{-1} sont les racines du polynôme $qX^2 - (p-2q)X + q \in \mathbb{Z}[X]$. Donc γ est un nombre algébrique de degré au plus 2 et p et q étant premiers entre eux, γ est une racine k-ième de l'unité si et seulement si $\phi(k) \leqslant 2$, i.e. $q = \pm 1$ et $|p - 2q| \leqslant 2$, ce qui correspond exactement aux cas exclus dans (3.1).

Clairement, si (α, β) est une paire de Lucas, quitte à changer (α, β) en une paire équivalente, on peut supposer $m > 0$ et comme $m = \sqrt{p}$, il vient :

$$(m, q) \notin \{(1, 1), (2, 1)\}. \tag{3.2}$$

Enfin, d'après l'assertion *1* de la proposition 2.1, si (α, β) est une paire de Lehmer, on a :

$$(\tilde{u}_n, q) = (\Phi_n, q) = (p, q) = 1. \tag{3.3}$$

3.2. Cas n = 2. Toute paire de **Lehmer** est 2-défectueuse car $\tilde{u}_2 = 1$.

Soit (α, β) une paire de **Lucas** 2-défectueuse. Comme $u_1 = 1$, tout nombre premier r divisant u_2 divise $(\alpha-\beta)^2$. Or avec les notations précédentes, il vient :

$$u_2 = \frac{\alpha^2 - \beta^2}{\alpha - \beta} = \alpha + \beta = m$$

et

$$(\alpha - \beta)^2 = (\alpha + \beta)^2 - 4\alpha\beta = m^2 - 4q.$$

Ainsi, m et q étant premiers entre eux, r ne peut qu'être égal a 2. Quitte à changer (α, β) en $(-\alpha, -\beta)$, on peut supposer que u_2 est positif. Il existe donc un entier naturel k tel que $u_2 = 2^k$. Le couple (a, b) associé à la paire (α, β) est donc de la forme $(2^k, 4^k - 4q)$.

On distingue alors les cas $k = 0$ et $k \geqslant 1$:

– $k = 0$: $(a, b) = (1, 1 - 4q)$ et (3.2) impose $q \neq 1$.

– $k \geqslant 1$: $(a, b) = (2^k, 4^k - 4q)$ et (3.3) impose $q \equiv 1 \bmod 2$.
Pour $k = 1$, (3.2) impose égalment $q \neq 1$.

3.3. Cas n = 3. Soit (α, β) une paire de **Lehmer** 3-défectueuse. On a $\tilde{u}_3 = p - q$. Comme $\tilde{u}_1 = \tilde{u}_2 = 1$, tout diviseur premier r de $\tilde{u}_3$ divise $(\alpha^2 - \beta^2)^2 = (\tilde{u}_3 + q)(\tilde{u}_3 - 3q)$. D'après (3.3), on a donc nécessairement $r = 3$. Quitte à remplacer (α, β) par $(i\alpha, i\beta)$, on peut supposer que $\tilde{u}_3 > 0$. Il existe donc $k \geqslant 0$ tel que $\tilde{u}_3 = 3^k$ et $p = 3^k + q$. Le couple $(a, b) = (p, p-4q)$ est donc de la forme $(3^k + q, 3^k - 3q)$.

– $k = 0$: $(a, b) = (1 + q, 1 - 3q)$ et (3.1) impose $q \neq 1$.

– $k \geqslant 1$: $(a, b) = (3^k + q, 3^k - 3q)$ et (3.3) impose $q \not\equiv 0 \bmod 3$.
Pour $k = 1$, (3.1) impose également $q \neq 1$.

Soit (α, β) une paire de **Lucas** 3-défectueuse. On a $u_3 = \tilde{u}_3 = m^2 - q$, mais contrairement au cas précédent, on ne peut pas supposer $u_3 > 0$. Donc $u_3 = \varepsilon 3^k$, $\varepsilon = \pm 1$, $k \geqslant 0$. Ainsi, (a, b) est de la forme $(m, 4\varepsilon 3^k - 3m^2)$.

– $k = 0$: si $\varepsilon = -1$, $(a, b) = (m, -4 - 3m^2)$.
En particulier, $m = 1$ **est permis.**
Si $\varepsilon = 1$, $(a, b) = (m, 4 - 3m^2)$ et $q \neq 0$ impose $m > 1$.

– $k \geqslant 1$: $(a, b) = (m, 4\varepsilon 3^k - 3m^2)$ et (3.3) impose $m \not\equiv 0 \bmod 3$.
Si $\varepsilon = k = 1$, (3.2) impose également $m \neq 2$.
En particulier, $\varepsilon = -1$ **permet** $(k, m) = (1, 2)$**.**

3.4. Cas n = 4. Soit (α, β) un paire de **Lehmer** 4-défectueuse. Comme $\tilde{u}_3 = p - q$ et $\tilde{u}_4 = p - 2q$, il vient $(\tilde{u}_3, \tilde{u}_4) = 1$ car $(p, q) = 1$. Tout diviseur r de $\tilde{u}_4$ divise donc $(\alpha^2 - \beta^2)^2 = (\tilde{u}_4 + 2q)(\tilde{u}_4 - 2q)$. Donc $r = 2$ et quitte à changer (α, β) en une paire équivalente, on peut supposer que $\tilde{u}_4 = 2^k$, $k \geqslant 0$. Le couple (a, b) est donc de la forme $(2^k + 2q, 2^k - 2q)$.

- $k = 0 : (a, b) = (1 + 2q, 1 - 2q)$ et (3.1) impose $q \neq 1$.
- $k \geqslant 1 : (a, b) = (2^k + 2q, 2^k - 2q)$ et (3.3) impose $q \equiv 1 \bmod 2$.
  Pour $k \in \{1, 2\}$, (3.1) impose également $q \neq 1$.

Soit (α, β) un paire de **Lucas** 4-défectueuse. C'est également une paire de Lehmer 4-défectueuse donc le seul diviseur premier de $\tilde{u}_4 = m^2 - 2q$ est 2. Mais l'on ne peut plus choisir le signe de $\tilde{u}_4$, donc $\tilde{u}_4 = \varepsilon 2^k$, $\varepsilon \in \{\pm 1\}$, $k \geqslant 0$. Le couple (a, b) est donc de la forme $(m, \varepsilon 2^{k+1} - m^2)$.

- $k = 0 : (a, b) = (m, 2\varepsilon - m^2)$ et $2q = m^2 - \varepsilon$ impose $m \equiv 1 \bmod 2$ et (3.2) impose $m \neq 1$.
- $k = 1 : (a, b) = (m, 4\varepsilon - m^2)$ et $2q = m^2 - 2\varepsilon$ impose $m \equiv 0 \bmod 2$.
  Si $\varepsilon = 1$, (3.2) impose également $m \neq 2$.
  En particulier, $\varepsilon = -1$ **permet** $m = 2$**.**
- Si $k > 1$, $2q = m^2 - 2^k\varepsilon$ impose $m \equiv q \equiv 0 \bmod 2$, ce qui est exclu.

3.5. Cas n = 5. Soit (α, β) une paire de **Lehmer** 5-défectueuse. D'après le critère cyclotomique, $\Phi_5 = (p - \eta^2 q)(p - \overline{\eta}^2 q) \in \{\pm 1, \pm 5\}$, où $\eta = \frac{1+\sqrt{5}}{2}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{5})$. Si $\Phi_5 = \pm 1$, $p - \eta^2 q$ est une unité. Il existe donc $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta^2 q = \varepsilon_0 \eta^{\varepsilon k}$. Si $\Phi_5 = \pm 5$, 5 se ramifie dans $\mathbb{Q}(\sqrt{5})$ donc $(5) = \mathfrak{p}^2$ où $\mathfrak{p} = (\sqrt{5})$. En notant $(p - \eta^2 q) = \prod_{i=1}^{s} \mathfrak{a}_i^{e_i}$, il vient :

$$\prod_{i=1}^{s} (\mathfrak{a}_i \overline{\mathfrak{a}}_i)^{e_i} = \mathfrak{p}^2.$$

Donc $s = 1$ et $\mathfrak{a}_1 = \overline{\mathfrak{a}}_1 = \mathfrak{p}$ et il existe $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta^2 q = \varepsilon_0 \sqrt{5} \eta^{k\varepsilon}$. Quitte à changer (α, β) en une paire équivalente, on a donc :

$$p - \eta^2 q = -\varepsilon(\varepsilon\eta^{\varepsilon})^k \tag{3.4}$$

ou

$$p - \eta^2 q = -\sqrt{5}(\varepsilon\eta^{\varepsilon})^k. \tag{3.5}$$

En considérant les équations conjuguées dans $\mathbb{Q}(\sqrt{5})$, il vient :

- (3.4) donne $p = \phi_{k-2\varepsilon}$, $q = \phi_k$, où (ϕ_k) est la suite de Fibonacci. Ainsi, $(a, b) = (\phi_{k-2\varepsilon}, \phi_{k-2\varepsilon} - 4\phi_k)$ et (3.1) impose $k \geqslant 3$.
- (3.5) donne $p = \psi_{k-2\varepsilon}$, $q = \psi_k$, où (ψ_k) est définie par $\psi_0 = 2, \psi_1 = 1, \psi_{k+2} = \psi_{k+1} + \psi_k$. On a alors $(a, b) = (\psi_{k-2\varepsilon}, \psi_{k-2\varepsilon} - 4\psi_k)$ et (3.1) impose $k \neq 1$.

3.6. Cas n = 6. Soit (α, β) une paire de **Lehmer** 6-défectueuse. On a $\tilde{u}_6 = p^2 - 4pq + 3q^2$. De plus, $(\tilde{u}_5, \tilde{u}_6) = 1$. En effet, $\tilde{u}_5 = p^2 - 3pq + q^2$, donc tout diviseur r de $(\tilde{u}_5, \tilde{u}_6)$ divise $\tilde{u}_6 - \tilde{u}_5 = q(2q - p)$. D'après (3.3), r divise $p - 2q$ donc r divise $(p-2q)^2 - \tilde{u}_6 = q^2$ et $r = 1$ toujours d'après (3.3). De même, $\tilde{u}_4 = p - 2q$, donc $(\tilde{u}_4, \tilde{u}_6) = 1$. Ainsi, comme $\Phi_6 = p - 3q$ divise $\tilde{u}_6$, tout diviseur r de Φ_6 divise $(\alpha^2 - \beta^2)^2 \tilde{u}_3 = (\Phi_6 + 3q)(\Phi_6 - q)(\Phi_6 + 2q)$. Toujours d'après (3.3), il vient $r \in \{2, 3\}$. Quitte à changer (α, β) en une paire équivalente, il existe donc $l, k \geqslant 0$ tels que $\Phi_6 = 2^k 3^l$ et (a, b) est de la forme $(2^k 3^l + 3q, 2^k 3^l - q)$.

- $l = k = 0 : (a, b) = (1 + 3q, 1 - q)$ et (3.1) impose $q \neq 1$.
- $l = 0,\ k \geqslant 1 : (a, b) = (2^k + 3q, 2^k - q)$ et $p = 2^k + 3q$ impose $p \equiv q \bmod 2$, donc (3.3) impose $q \equiv 1 \bmod 2$.
  Pour $k = 1$, (3.1) impose $q \neq -1$.
- $l \geqslant 1,\ k = 0 : (a, b) = (3^l + 3q, 3^l - q)$. $p = 3^l + 3q$ impose $q \not\equiv 0 \bmod 3$.
  Pour $l = 1$, (3.1) impose $q \neq -1$.
- $l \geqslant 1,\ k \geqslant 1 : (a, b) = (2^k 3^l + 3q, 2^k 3^l - q)$ et $p = 2^k 3^l + 3q$ impose $q \equiv \pm 1 \bmod 6$.

Soit (α, β) une paire de **Lucas** 6-défectueuse. C'est également une paire de Lehmer 6-défectueuse, mais comme plus haut, on ne peut choisir le signe de Φ_6. Donc $\Phi_6 = \varepsilon 2^k 3^l = m^2 - 3q$ et (a, b) est de la forme $(m, \frac{1}{3}(\varepsilon 2^{k+2} 3^l - m^2))$.

- $l = 0,\ k = 0 : m^2 = \varepsilon + 3q \equiv \varepsilon \bmod 3$ et comme -1 n'est pas un carré modulo 3, il vient $\varepsilon = 1$ et $m \not\equiv 0 \bmod 3$. De plus, $q = \frac{1}{3}(m^2 - 1)$ donc (3.1) impose $m \neq 1$ et $m \neq 2$. On a donc $(a, b) = (m, \frac{1}{3}(4 - m^2))$ avec $m \geqslant 4,\ m \not\equiv 0 \bmod 3$.
- $l = 0,\ k \geqslant 1 : m^2 - 3q = 2^k \varepsilon$, donc $m \equiv q \bmod 2$ et (3.3) impose $m \equiv 1 \bmod 2$. De plus, $m^2 \equiv (-1)^k \varepsilon \bmod 3$ donc $\varepsilon = (-1)^k$ et $m \not\equiv 0 \bmod 3$.
  On a donc $(a, b) = (m, \frac{1}{3}((-2)^{k+2} - m^2))$, $m \equiv \pm 1$ mod 6 et pour $k = 1$, (3.2) impose $m \neq 1$.
- $l = 1 : (a, b) = (m, 2^{k+2}\varepsilon - \frac{m^2}{3})$ et $m^2 = \varepsilon 3.2^k + 3q$ impose $m \equiv 0 \bmod 3$. Pour $k \geqslant 1$, $m \equiv q \bmod 2$ donc (3.3) impose $m \equiv 1 \bmod 2$, i.e. $m \equiv 3 \bmod 6$.
- $l > 1 : m \equiv 0 \bmod 3$ donc 9 divise $3q = m^2 - \varepsilon 2^k 3^l$ et donc 3 divise (m, q) ce qui est exclu.

3.7. Cas n = 8. Soit (α, β) une paire de **Lehmer** 8-défectueuse. D'après le critère cyclotomique, $\Phi_8 = (p - q\eta\sqrt{2})(p - q\overline{\eta}\sqrt{2}) \in \{\pm 1, \pm 2\}$, où $\eta = 1 + \sqrt{2}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$. Comme dans le cas $n = 5$, comme 2 se ramifie dans $\mathbb{Q}(\sqrt{2})$, quitte à changer (α, β) en une paire équivalente, il existe $\varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tel que

$$p - q\eta\sqrt{2} = -\varepsilon(\varepsilon\eta^{\varepsilon})^k \tag{3.6}$$

ou

$$p - q\eta\sqrt{2} = -\sqrt{2}(\varepsilon\eta^{\varepsilon})^k. \tag{3.7}$$

En considérant les équations conjuguées dans $\mathbb{Q}(\sqrt{2})$, il vient :

- l'équation (3.6) donne $p = \rho_{k-\varepsilon}$, $q = \pi_k$, où (ρ_k) est définie par $\rho_0 = \rho_1 = 1$ et $\rho_{k+2} = 2\rho_{k+1}+\rho_k$ et (π_k) est donnée par $\pi_0 = 0$, $\pi_1 = 1$ et $\pi_{k+2} = 2\pi_{k+1} + \pi_k$. Donc $(a, b) = (\rho_{k-\varepsilon}, \rho_{k-\varepsilon} - 4\pi_k)$.
- l'équation (3.7) donne $p = 2\pi_{k-\varepsilon}$, $q = \rho_k$ et $(a, b) = (2\pi_{k-\varepsilon}, 2\pi_{k-\varepsilon} - 4\rho_k)$.

Dans les deux cas, (3.1) impose $k \geqslant 2$.

3.8. Cas n = 10. Pour tout couple (α, β), $\Phi_{10}(\alpha, \beta) = \Phi_5(-\alpha, \beta)$. Ainsi, si (α, β) est une paire de **Lehmer** 10-défectueuse, d'après le critère cyclotomique, il vient :

$$\Phi_{10}(\alpha, \beta) = \Phi_5(-\alpha, \beta) = (p' - \eta^2 q')(p' - \overline{\eta}^2 q') \in \{\pm 1, \pm 5\}$$

où $q' = -\alpha\beta = -q$ et $p' = (-\alpha + \beta)^2 = p + 4q$. D'après l'étude du cas $n = 5$, on a donc :

- $p = p' + 4q' = \phi_{k-2\varepsilon} + 4\phi_k$, $q = -q' = -\phi_k$. Donc $(a, b) = (\phi_{k-2\varepsilon} + 4\phi_k, \phi_{k-2\varepsilon})$ et (3.1) impose $k \geqslant 3$.
- $p = p' + 4q' = \psi_{k-2\varepsilon} + 4\psi_k$, $q = -q' = -\psi_k$. Donc $(a, b) = (\psi_{k-2\varepsilon} + 4\psi_k, \psi_{k-2\varepsilon})$ et (3.1) impose $k \neq 1$.

3.9. Cas n = 12. Soit (α, β) une paire de **Lehmer** 12-défectueuse. D'après le critère cyclotomique,

$$\Phi_{12} = (p - q\eta)(p - q\overline{\eta}) \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

où $\eta = 2 + \sqrt{3}$ est l'unité fondamentale de $\mathbb{Q}(\sqrt{3})$. Si $\Phi_{12} = \pm 1$, $p - \eta q$ est une unité. Il existe donc $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0\eta^{\varepsilon k}$. Si $\Phi_{12} = \pm 3$, comme 3 se ramifie dans $\mathbb{Q}(\sqrt{3})$, il existe $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0\sqrt{3}\eta^{\varepsilon k}$. Si $\Phi_{12} = \pm 2$, en notant $\theta = 1 + \sqrt{3}$, on a $\overline{\theta} = \theta\overline{\eta}$. Donc 2 se ramifie dans $\mathbb{Q}(\sqrt{3})$ et comme pour le cas $n = 5$, $p - \eta q$ est associé a θ. Il existe donc $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0\theta\eta^{\varepsilon k}$. Enfin, si $\Phi_{12} = \pm 6$, il existe $\varepsilon_0, \varepsilon \in \{\pm 1\}$ et $k \geqslant 0$ tels que $p - \eta q = \varepsilon_0\theta\sqrt{3}\eta^{\varepsilon k}$. Quitte à remplacer (α, β) par une paire équivalent, on a donc :

$$p - \eta q = -\varepsilon\eta^{\varepsilon k} \tag{3.8}$$

$$p - \eta q = -\sqrt{3}\eta^{\varepsilon k} \tag{3.9}$$

$$p - \eta q = -\varepsilon\theta\eta^{\varepsilon k} \tag{3.10}$$

ou

$$p - \eta q = -\sqrt{3}\theta\eta^{\varepsilon k} \tag{3.11}$$

En considérant les équations conjuguées, il vient $p = \zeta^{(i)}_{k-\varepsilon}$, $q = \zeta^{(i)}_k$, $i \in \{0,1,2,3\}$ où les suites $(\zeta^{(i)}_k)$ sont définies par $\zeta^{(i)}_{k+1} = 4\zeta^{(i)}_k - \zeta^{(i)}_{k-1}$ et les valeurs initiales suivantes :

i	0	1	2	3
$\zeta^{(i)}_0$	0	1	ε	1
$\zeta^{(i)}_1$	1	2	$2\varepsilon+1$	$3\varepsilon+2$

Par ailleurs, $p-4q = \zeta^{(i)}_{k-\varepsilon} - 4\zeta^{(i)}_k = -\zeta^{(i)}_{k+\varepsilon}$. Donc $(a,b) = (\zeta^{(i)}_{k-\varepsilon}, -\zeta^{(i)}_{k+\varepsilon})$ et (3.1) impose $(i,k) \notin \{(0,0),(0,1),(1,0),(2,0)\}$ et si $\varepsilon = -1$, $(i,k) \neq (2,1)$.

4. Conclusion

On a démontré le théorème suivant :

Théorème 4.1. *Toute paire de Lucas est* 1*-défectueuse et toute paire de Lehmer est* 1*- et* 2*-défectueuse.*

Pour $n \in \{2,3,4,6\}$, à équivalence près, toute paire de Lucas n-défectueuse est de la forme $((a+\sqrt{b})/2, (a-\sqrt{b})/2)$ où (a,b) est donné dans la table ci- dessous.

n	(a,b)	
2	$(1, 1-4q)$, $q \neq 1$	$(2^k, 4^k - 4q)$, $k > 0$, $q \equiv 1 \ mod\ 2$, $(k,q) \neq (1,1)$
3	$(m, -4-3m^2)$,	$(m, 4.3^k\varepsilon - 3m^2)$, $m \not\equiv 0 \ mod\ 3$, $k > 0$,
	$(m, 4-3m^2)$, $m > 1$	$(\varepsilon, k, m) \neq (1,1,2)$
4	$(m, 2\varepsilon - m^2)$, $m \equiv 1 \ mod\ 2$, $m \neq 1$	$(m, 4\varepsilon - m^2)$, $m \equiv 0 \ mod\ 2$, $(\varepsilon, m) \neq (1,2)$
6	$(m, (4-m^2)/3)$, $m \not\equiv 0 \ mod\ 3$, $m > 3$	$(m, ((-2)^{k+2} - m^2)/3)$, $k > 0$, $m \equiv \pm 1 \ mod\ 6$, $(k,m) \neq (1,1)$
	$(m, 4\varepsilon - m^2/3)$, $m \equiv 0 \ mod\ 3$	$(m, 2^{k+2}\varepsilon - m^2/3)$, $k > 0$, $m \equiv 3 \ mod\ 6$

Pour $n \in \{3,4,5,6,8,10,12\}$, à équivalence près, toute paire de Lehmer n-défectueuse est de la forme $((\sqrt{a}+\sqrt{b})/2, (\sqrt{a}-\sqrt{b})/2)$ où (a,b) est donné dans la table ci-après.

n	(a,b)	
3	$(1+q, 1-3q)$, $q \neq 1$	$(3^k, 3^k-3q)$, $k>0$, $q \not\equiv 0 \ mod\ 3$, $(k,q) \neq (1,1)$
4	$(1+2q, 1-2q)$, $q \neq 1$	$(2^k+2q, 2^k-2q)$, $k>0$, $q \equiv 1 \ mod\ 2$, $(k,q) \notin \{(1,1),(2,1)\}$
5	$(\phi_{k-2\varepsilon}, \phi_{k-2\varepsilon}-4\phi_k)$, $k>2$	$(\psi_{k-2\varepsilon}, \psi_{k-2\varepsilon}-4\psi_k)$, $k \neq 1$
6	$(1+3q, 1-q)$, $q \neq 1$	$(2^k+3q, 2^k-q)$, $k>0$, $q \equiv 1 \ mod\ 2$, $(k,q) \neq (1,-1)$
	$(3^l+3q, 3^l-q)$, $l>0$, $q \not\equiv 0 \ mod\ 3$, $(l,q) \neq (1,-1)$	$(2^k3^l+3q, 2^k3^l-q)$, $k,l>0$, $q \equiv \pm 1 \ mod\ 6$
8	$(\rho_{k-\varepsilon}, \rho_{k-\varepsilon}-4\pi_k)$, $k>1$	$(2\pi_{k-\varepsilon}, 2\pi_{k-\varepsilon}-4\rho_k)$, $k>1$
10	$(\phi_{k-2\varepsilon}+4\phi_k, \phi_{k-2\varepsilon})$, $k>2$	$(\psi_{k-2\varepsilon}+4\psi_k, \psi_{k-2\varepsilon})$, $k \neq 1$
12	$(\zeta^{(i)}_{k-\varepsilon}, -\zeta^{(i)}_{k+\varepsilon})$, $(i,k) \notin \{(0,0),(0,1),(1,0),(2,0)\}, (i,k,\varepsilon) \neq (2,1,-1)$	

Rappelons que les suites (ϕ_k) *et* (ψ_k) *sont définies au paragraphe 3.5, les suites* (ρ_k) *et* (π_k) *sont définies au paragraphe 3.7 et les suites* $(\zeta^{(i)}_k)$, $i = 0,1,2,3$ *sont définies au paragraphe 3.9.*

Bibliographie

[1] Y. Bilu, G. Hanrot, P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*. J. reine angew. Math. **539** (2001), 75–122.

[2] P.D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$. Ann. Math. (2) **15** (1913), 30–70.

[3] L. K. Durst, *Exceptional real Lehmer sequences*. Pacific J. Math. **9** (1959), 437–41.

[4] D. H. Lehmer, *An extended theory of Lucas' functions*. Ann. of Math. (2) **31** (1930), 419–48.

[5] E. Lucas, *Sur les rapports qui existent entre la théorie des nombres et le calcul intergal*. C. R. Acad. Sci. Paris **82** (1876), 1303–5.

[6] E. Lucas, *Théorie des fonctions numériques simplement périodiques*. Amer. J. Math. **1** (1878), 184–240, 289–321.

[7] A. Schinzel, *The intrinsic divisors of Lehmer numbers I*. Acta Arith. **8** (1963), 213–23.

[8] C. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*. Proc. London Math. Soc. (3) **35** (1997), 425–447.

[9] P.M. Voutier, *Primitive divisors of Lucas ans Lehmer sequences*. Math. Comp. **64** (1995), 869–888.

[10] M. Ward, *The intrinsic divisors of Lehmer numbers*. Ann. of Math. (2) **62** (1955), 230–36.

[11] K. Zsigmondy, *Zur Theorie der Potenzreste*. Moantsh. Math. **3** (1892), 265–284.

Mourad Abouzaid
Université Bordeaux 1
351, cours de la Libération
33405 Talence Cedex, France
E-mail : Mourad.Abouzaid@math.u-bordeaux1.fr
URL: http ://www.math.u-bordeaux1.fr/A2X/