Sur les bonnes valeurs initiales de la suite de Lucas-Lehmer

Bruno DESCHAMPS

Université du Maine

Résumé.— Dans cet article nous explicitons une infinité de *bonnes de valeurs initiales* pour la suite de Lucas-Lehmer.

Abstract.— In this article we give an infinite number of good initial values for the Lucas-Lehmer sequence.

1.— Introduction et notations.

Les nombres de Mersenne sont les entiers de la forme 2^p-1 avec p premier. Si a est un entier naturel tel que 2^a-1 soit un nombre premier alors a est lui-même premier. Toutefois, tous les nombres de Mersenne ne sont pas premiers, par exemple $2^{11}-1 = 23\times 89$. Lucas a proposé un test, simplifié par Lehmer en 1930, pour caractériser les premiers p tels que 2^p-1 soit un nombre premier : on considère une suite récurrente $(u_n)_n$ vérifiant pour tout $n\geq 0$, $u_{n+1}=u_n^2-2$. Si on a $u_0=4$ alors pour tout premier $p\geq 3$

$$2^p-1 \text{ est premier} \Longleftrightarrow 2^p-1 \text{ divise } u_{p-2} \quad (*)$$

Si l'on considère une autre valeur initiale $u_0\in\mathbb{Z}$ pour $(u_n)_n$ alors la condition 2^p-1 *divise* u_{p-2} reste suffisante pour assurer la primalité de 2^p-1 (voir corollaire 2), mais peut perdre sont caractère nécessaire : par exemple si l'on prend $u_0=5$ et $p=3$ alors on voit que $2^p-1=7$, bien qu'étant un nombre premier, ne divise pas $u_1=23$. Dans cet article on s'intéresse aux valeurs initiales u_0 de cette suite pour lesquelles la condition reste nécessaire et suffisante. Dans la suite, nous appelerons *suite de Lucas-Lehmer* toute suite à valeurs entières $(u_n)_n$ vérifiant la relation $u_{n+1}=u_n^2-2$ et *bonne valeur initiale de la suite de Lucas-Lehmer pour* $p\geq p_0$ tout entier $u_0\in\mathbb{N}$ tel que l'équivalence $(*)$ soit vérifiée pour tout $p\geq p_0$ premier (ici p_0 sera explicite).

Nous apportons quelques précisions sur le test de primalité de Lucas-Lehmer, en particulier nous montrons que pour toute valeur initiale u_0 et tout 2^p-1 premier, ce dernier divise au plus un terme de la suite $(u_n)_n$ et que si ce terme n'est pas celui d'indice $p-2$ alors la suite $(u_n)_n$ est obtenue, modulo 2^p-1, par translation d'une autre suite de Lucas-Lehmer.

Nous caractérisons ensuite par des symboles de Legendre les bonnes valeurs intiales de la suite de Lucas-Lehmer : un entier $u_0\in\mathbb{Z}$ est une bonne valeur initiale si et seulement si pour tout q nombre premier de Mersenne assez grand, on a simultanément $\left(\frac{u_0-2}{q}\right)=1$ et $\left(\frac{u_0+2}{q}\right)=-1$ (corollaire 5). Cette caractérisation, permet de faire correspondre les bonnes valeurs initiales de la suite de Lucas-Lehmer aux points entiers de certaines courbes que nous décrivons (proposition 6). Une application machine permet d'expliciter certaines de ces courbes. Une étude détermine alors les points entiers de deux d'entre elles et permet alors de leur associer deux ensembles infinis de bonne valeurs initiales de la suite de Lucas-Lehmer.

[0]2000 Mathematics Subject Classification : Primary 11P99 Secondary 11A99, 11P32

De manière précise, nous trouvons finalement que si l'on considère les deux suites récurrentes $(x_n)_n$ et $(y_n)_n$ définies par

$$\begin{cases} x_0 = 1,\ x_1 = 5 & \text{et pour tout } n \geq 0 \quad x_{n+2} = 4x_{n+1} - x_n \\ y_0 = 1,\ y_1 = 9 & \text{et pour tout } n \geq 0 \quad y_{n+2} = 10y_{n+1} - y_n \end{cases}$$

alors les deux familles d'entiers

- $\left\{2x_n^2 + 2/\ n \in \mathbb{N}\right\}$
- $\left\{12y_n^2 - 2/\ n \in \mathbb{N}\right\}$

sont des familles de bonnes valeurs initiales de la suite de Lucas-Lehmer pour $p \geq 3$ (le cas historique, $u_0 = 4$, est en fait la première valeur de la première famille décrite ici).

2.— Test de primalité des nombres de Mersenne

2.1.— Suffisance du critère de divisibilité. L'idée développée dans cette partie est bien connue (cf [B], voir aussi [R]). Nous la rappelons, car c'est l'idée directrice pour l'étude des bonnes valeurs initiales que nous proposons.

On considère un corps commutatif K et on note $\overline{K}$ sa clôture algébrique. Soit $(\lambda_n)_n$ une suite d'éléments de K vérifiant pour tout $n \geq 0$, $\lambda_{n+1} = \lambda_n^2 - 2$. Une récurrence immédiate montre que pour tout $n \geq 0$ on a $\lambda_n = \alpha^{2^n} + \beta^{2^n}$ où $\alpha, \beta \in \overline{K}$ désignent les deux racines du polynôme $P(x) = X^2 - \lambda_0 X + 1 \in K[X]$.

Ainsi, si l désigne un nombre premier et si $(u_n)_n$ est une suite de Lucas-Lehmer alors la suite $(\overline{u_n})_n$ des résidus modulo l de la suite $(u_n)_n$ vérifie pour tout $n \geq 0$

$$\overline{u_n} = \alpha^{2^n} + \beta^{2^n}$$

où $\alpha, \beta \in \overline{\mathbb{F}}_l$ désignent les deux racines du polynôme $P(x) = X^2 - \overline{u_0}X + 1 \in \mathbb{F}_l[X]$. En particulier, on voit que pour tout indice $k \geq 0$, on a :

$$l | u_k \Longleftrightarrow \alpha^{2^k} + \beta^{2^k} = 0$$

Dans la suite de ce texte, p désignera toujours un nombre premier, q un nombre premier de Mersenne et $(u_n)_n$ une suite de Lucas-Lehmer. Nous commençons par établir un lemme qui montre que les termes de la suite $(u_n)_n$ ne possèdent pas de petits diviseurs impairs :

Lemme 1.— *Soit $k \geq 0$ un indice et $l \geq 3$ un nombre premier. Si l divise u_k alors $l > 2^{\frac{k+2}{2}}$.*

Preuve : On se place dans $\overline{\mathbb{F}}_l$ et on note α et β les deux racines de $P(X) = X^2 - \overline{u_0}X + 1$. On a $l | u_k \Longleftrightarrow \alpha^{2^k} + \beta^{2^k} = 0 \Longleftrightarrow \alpha^{2^{k+1}} = -1 \Longleftrightarrow o(\alpha) = 2^{k+2}$. Maintenant P étant de degré 2, on a $\alpha \in \mathbb{F}_{l^2}$ et comme $o(\mathbb{F}_{l^2}) = l^2 - 1$ on a $2^{k+2} \leq (l^2 - 1)$. Ceci conduit à $l > 2^{\frac{k+2}{2}}$.

Corollaire 2.— *Si $2^p - 1$ divise u_{p-2} alors $2^p - 1$ est premier.*

Preuve : Considérons un premier $l \leq \sqrt{2^p - 1}$. Si $l | (2^p - 1) | u_{p-2}$ alors $l \geq 3$ et, d'après le lemme précédent, on a $l > 2^{\frac{p}{2}}$, ce qui est absurde. Ainsi l'entier $2^p - 1$ ne possède pas de diviseur premier inférieur à sa racine carrée, il est donc premier.

2.2.— Etude de la réciproque. Dans ce paragraphe on se donne un nombre premier p tel que $q = 2^p - 1$ soit premier. On considère une valeur initiale $u_0 \in \mathbb{Z}$ de la suite de Lucas-Lehmer. On note α, β les racines dans $\overline{\mathbb{F}}_q$ du polynôme $P(X) = X^2 - \overline{u_0}X + 1 \in \mathbb{F}_q[X]$.

Lemme 3.— *Le premier q divise le terme u_n de la suite de Lucas-Lehmer si et seulement si $o(\alpha) = 2^{n+2}$ dans $\overline{\mathbb{F}}_q^*$.*

Preuve : On a $q|u_n \iff \overline{u_n} = 0 \iff \alpha^{2^n} + \beta^{2^n} = 0 \iff \alpha^{2^{n+1}} = -1 \iff o(\alpha) = 2^{n+2}$.

Théorème 4.— *On pose $u = u_0^2 - 4$.*

- *Si $\left(\frac{u}{q}\right) = 0$ ou 1 alors q ne divise aucun terme de la suite $(u_n)_n$.*
- *Si $\left(\frac{u}{q}\right) = -1$, on considère une suite d'éléments de $\overline{\mathbb{F}}_q^*$, $(\lambda_n)_n$, définie par*

$$\lambda_0 = \overline{u_0},\ \forall n \geq 0,\ \lambda_{n+1} = \sqrt{\lambda_n + 2}$$

(où $\sqrt{.}$ désigne n'importe quelle détermination de la racine carrée dans $\overline{\mathbb{F}}_q^*$)

Il existe alors un indice h tel que

$$\lambda_0, \cdots, \lambda_h \in \mathbb{F}_q \text{ et } \lambda_{h+1} \notin \mathbb{F}_q$$

On a $o(\alpha) = 2^{p-h}$ et, par suite, $q|u_{p-h-2}$.

Preuve : • Si $\left(\frac{u}{q}\right) = 0$ ou 1 alors le polynôme $P(X)$ est réductible sur $\mathbb{F}_q[X]$ et donc $\alpha \in \mathbb{F}_q$, donc $o(\alpha)|o(\mathbb{F}_q^*) = q - 1 = 2(2^{p-1} - 1)$, il s'ensuit que l'équation $o(\alpha) = 2^{n+2}$ n'a pas de solution dans $\mathbb{N}$ ce qui implique, par le lemme 3, que q ne divise aucun terme de la suite $(u_n)_n$.

• Si $\left(\frac{u}{q}\right) = -1$, alors P est irréductible sur $\mathbb{F}_q[X]$ et donc α est quadratique sur $\mathbb{F}_q$, c'est-à-dire que $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^2}$. On a

$$\alpha = \frac{\overline{u_0} + \sqrt{\overline{u}}}{2}$$

On a donc

$$\alpha^{2^p} = \alpha.\left(\frac{\overline{u_0} + \sqrt{\overline{u}}}{2}\right)^q = \alpha.\frac{\overline{u_0}^q + \sqrt{\overline{u}}^q}{2^q}$$

Comme $2, \overline{u_0} \in \mathbb{F}_q$, on a $2^q = 2$ et $\overline{u_0}^q = \overline{u_0}$. Par ailleurs, on a

$$\sqrt{\overline{u}}^q = \sqrt{\overline{u}}.\sqrt{\overline{u}}^{q-1} = \sqrt{\overline{u}}.\overline{u}^{\frac{q-1}{2}} = \left(\frac{u}{q}\right)\sqrt{\overline{u}} = -\sqrt{\overline{u}}$$

On en déduit donc que

$$\alpha^{2^p} = \left(\frac{\overline{u_0} + \sqrt{\overline{u}}}{2}\right).\left(\frac{\overline{u_0} - \sqrt{\overline{u}}}{2}\right) = \frac{\overline{u_0}^2 - \overline{u}}{4} = 1$$

et, par suite, l'ordre de α est de la forme 2^k avec $k \leq p$.

Considérons dans $\overline{\mathbb{F}}_q$ la suite $(\sqrt[2^i]{\alpha})_{i\geq 1}$ et montrons par récurrence sur i que l'on a

$$\sqrt[2^i]{\alpha} = \frac{\lambda_i}{2} + \frac{1}{2\lambda_1.\cdots.\lambda_i}\sqrt{u}$$

Pour $i = 1$ on a

$$\left(\frac{\sqrt{\overline{u_0}+2}}{2} + \frac{1}{2\sqrt{\overline{u_0}+2}}\sqrt{u}\right)^2 = \frac{\overline{u_0}+2}{4} + \frac{\overline{u_0}^2-4}{4(\overline{u_0}+2)} + \frac{\sqrt{u}}{2} = \frac{\overline{u_0}}{2} + \frac{\sqrt{u}}{2} = \alpha$$

Supposons la propriété vraie pour $i \geq 1$, alors pour $i+1$ on a

$$\left(\frac{\lambda_{i+1}}{2} + \frac{1}{2\lambda_1.\cdots.\lambda_{i+1}}\sqrt{u}\right)^2 = \left(\frac{\lambda_{i+1}^2}{4} + \frac{u}{4\lambda_1^2.\cdots.\lambda_{i+1}^2}\right) + \frac{1}{2\lambda_1.\cdots.\lambda_i}\sqrt{u}$$

Remarquons maintenant que

$$\begin{array}{rclcl} u & = & \overline{u_0}^2 - 4 & = & (\lambda_0+2)(\lambda_0-2) \\ & = & \lambda_1^2(\lambda_1^2-4) & = & \lambda_1^2(\lambda_1+2)(\lambda_1-2) \\ & \vdots & & & \\ & = & \lambda_1^2\cdots\lambda_{i+1}^2(\lambda_{i+1}^2-4) & & \end{array}$$

on a donc

$$\begin{array}{rcl} \left(\frac{\lambda_{i+1}}{2} + \frac{1}{2\lambda_1.\cdots.\lambda_{i+1}}\sqrt{u}\right)^2 & = & \frac{2\lambda_{i+1}^2-4}{4} + \frac{1}{2\lambda_1.\cdots.\lambda_i}\sqrt{u} \\ & = & \frac{\lambda_i}{2} + \frac{1}{2\lambda_1.\cdots.\lambda_i}\sqrt{u} \\ & = & \sqrt[2^i]{\alpha} \end{array}$$

On en déduit que si $\lambda_0, \cdots, \lambda_i \in \mathbb{F}_q$ alors $\sqrt[2^i]{\alpha} \in \mathbb{F}_{q^2}$.

Comme $\alpha \neq 1$ est d'ordre une puissance de 2, on a pour tout $i \geq 1$, $o(\sqrt[2^i]{\alpha}) = 2^{i+k}$. Ainsi, la suite $(\sqrt[2^i]{\alpha})_{i\geq 1}$ ne peut pas être toujours à valeurs dans $\mathbb{F}_{q^2}$, sinon il y aurait des éléments d'ordre arbitrairement grand dans $\mathbb{F}_{q^2}^*$, ce qui est absurde. On en déduit que la suite $(\lambda_i)_i$ ne peut pas être toujours à valeurs dans $\mathbb{F}_q$, ce qui montre l'existence de l'entier h annoncé dans le théorème. Montrons que cet entier h est l'entier tel que

$$\sqrt[2^{h+1}]{\alpha} \in \mathbb{F}_{q^2}^* \text{ et } \sqrt[2^{h+2}]{\alpha} \notin \mathbb{F}_{q^2}^*$$

<u>1er cas : $h = 0$.</u> On a donc $\left(\frac{\overline{u_0}+2}{q}\right) = -1$ et comme $-1 = \left(\frac{\overline{u_0}+2}{q}\right)\left(\frac{\overline{u_0}-2}{q}\right)$ on en déduit que $\left(\frac{\overline{u_0}-2}{q}\right) = 1$ et donc $\sqrt{\overline{u_0}-2} \in \mathbb{F}_q^*$. On a alors

$$\sqrt{\alpha} = \frac{\sqrt{\overline{u_0}-2}}{2} + \frac{1}{2\sqrt{\overline{u_0}-2}}\sqrt{u} \in \mathbb{F}_{q^2}^*$$

Supposons que $\sqrt[4]{\alpha} \in \mathbb{F}_{q^2}^*$, il existe donc $x, y \in \mathbb{F}_q$ tels que

$$(x + y\sqrt{u})^2 = \frac{\sqrt{\overline{u_0}-2}}{2} + \frac{1}{2\sqrt{\overline{u_0}-2}}\sqrt{u}$$

ce qui équivaut au système

$$\left\{\begin{array}{rcl} xy & = & \frac{1}{4\sqrt{\overline{u_0}-2}} \\ x^2 + y^2u & = & \frac{\sqrt{\overline{u_0}-2}}{2} \end{array}\right.$$

En substituant, ce système implique que x est solution de l'équation

$$16(\overline{u_0}-2)x^4-8(\overline{u_0}-2)^{3/2}x^2+\overline{u}=0$$

Le discriminant Δ de cette équation doit donc être un carré dans $\mathbb{F}_q$, or

$$\Delta=64(\overline{u_0}-2)^3-64(\overline{u_0}-2)^2(\overline{u_0}+2)=-[16(\overline{u_0}-2)]^2$$

donc -1 est un carrée dans $\mathbb{F}_q$, or $\left(\frac{-1}{q}\right)=(-1)^{\frac{q-1}{2}}=(-1)^{2^{p-1}-1}=-1$, ce qui est absurde.

2ème cas : $h\geq 1$. D'après ce qui précède, on a

$$\sqrt[2^h]{\alpha}=\frac{\lambda_h}{2}+\frac{1}{2\lambda_1.\cdots.\lambda_h}\sqrt{\overline{u}}$$

Par hypothèse, λ_h+2 n'est pas un carré dans $\mathbb{F}_q$, on en déduit que λ_h-2 est un carré dans $\mathbb{F}_q$. En effet on a

$$-1=\left(\frac{u}{q}\right)=\left(\frac{u_0^2-4}{q}\right)=\left(\frac{u_0-2}{q}\right)\left(\frac{u_0+2}{q}\right)=\left(\frac{u_0-2}{q}\right)$$

et par suite on a

$$\begin{aligned}
-1 &= \left(\frac{\lambda_0-2}{q}\right)=\left(\frac{\lambda_1^2-4}{q}\right)=\left(\frac{\lambda_1-2}{q}\right)\left(\frac{\lambda_1+2}{q}\right)\\
&= \left(\frac{\lambda_1-2}{q}\right)=\left(\frac{\lambda_2^2-4}{q}\right)=\left(\frac{\lambda_2-2}{q}\right)\left(\frac{\lambda_2+2}{q}\right)\\
&\vdots\\
&= \left(\frac{\lambda_{h-1}-2}{q}\right)=\left(\frac{\lambda_h^2-4}{q}\right)=\left(\frac{\lambda_h-2}{q}\right)\left(\frac{\lambda_h+2}{q}\right)
\end{aligned}$$

et donc $\left(\frac{\lambda_h-2}{q}\right)=1$. On a alors

$$\sqrt[2^{h+1}]{\alpha}=\frac{\sqrt{\lambda_h-2}}{2}+\frac{1}{2\lambda_1.\cdots.\lambda_h.\sqrt{\lambda_h-2}}\sqrt{\overline{u}}\in\mathbb{F}_{q^2}^*$$

Supposons que $\sqrt[2^{h+2}]{\alpha}\in\mathbb{F}_{q^2}^*$, il existe donc $x,y\in\mathbb{F}_q$ tels que

$$(x+y\sqrt{\overline{u}})^2=\frac{\sqrt{\lambda_h-2}}{2}+\frac{1}{2\lambda_1.\cdots.\lambda_h.\sqrt{\lambda_h-2}}\sqrt{\overline{u}}$$

ce qui équivaut au système

$$\begin{cases}
xy &= \dfrac{1}{4\lambda_1.\cdots.\lambda_h\sqrt{\lambda_h-2}}\\
x^2+y^2u &= \dfrac{\sqrt{\lambda_h-2}}{2}
\end{cases}$$

En substituant, ce système implique que x est solution de l'équation

$$16x^4-8\sqrt{\lambda_h-2}.x^2+(\lambda_h+2)=0$$

Le discriminant de cette équation vaut -256, on en déduit donc que -1 est un carré dans $\mathbb{F}_q$ ce qui est absurde.

Puisque α est d'ordre une puissance de 2, il appartient au 2-Sylow de $\mathbb{F}_{q^2}^*$. Ce sous-groupe est cyclique d'ordre 2^{p+1} puisque $\mathbb{F}_{q^2}^*$ est cyclique et que $o(\mathbb{F}_{q^2}^*) = q^2 - 1 = 2^{p+1}(2^{p-1}-1)$. Comme $\sqrt[2^{h+1}]{\alpha} \in S_2$ on en déduit qu'il existe un entier $l \leq 2^{p+1}$ tel que $\sqrt[2^{h+1}]{\alpha} = t^l$ où t désigne un générateur de S_2. On a donc $\alpha^{2^{p-h}} = t^{l2^{p+1}} = 1$ et par suite $o(\alpha) \leq 2^{p-h}$. Si $o(\alpha) < 2^{p-h}$ alors $o(\alpha) \leq 2^{p-h-1}$ et donc $\alpha^{2^{p-h-1}} = 1$, ainsi $t^{l2^p} = 1$ mais comme $o(t) = 2^{p+1}$ on en déduit qu'il existe un entier $l^{'}$ tel que $l = 2l^{'}$ et donc $t^{l^{'}} = \sqrt[2^{h+2}]{\alpha} \in \mathbb{F}_{q^2}^*$ ce qui est absurde. Donc $o(\alpha) = 2^{p-h}$ et donc, d'après le lemme 3, $q|u_{p-h-2}$.

Corollaire 5.— *1/ Le premier q divise au maximum un terme d'une suite de Lucas-Lehmer et, dans le cas où il en divise un, l'indice de ce terme est $\leq p-2$.*

2/ Si q divise le terme u_k d'une suite de Lucas-Lehmer $(u_n)_n$ alors il existe une autre suite de Lucas-Lehmer $(v_n)_n$ telle que pour tout $n \geq p-2-k$, $\overline{v_n} = \overline{u_{n+k-(p-2)}}$.

3/ On a l'équivalence

$$q|u_{p-2} \Longleftrightarrow \left(\frac{u_0-2}{q}\right) = 1 \ et \ \left(\frac{u_0+2}{q}\right) = -1$$

Preuve : 1/ Comme l'ordre de α est unique, le lemme 3 montre que q divise au maximum un seul élément d'une suite de Lucas-Lehmer. On a vu dans la preuve du théorème précédent que si q divise un terme u_k d'une suite de Lucas-Lehmer, alors $\alpha^{2^p} = 1$ et donc, d'après le lemme 3, on a $k+2 \leq p$.

2/ On reprend les notations du théorème précédent. Puisque $q|u_k$, c'est le seul terme de la suite $(u_n)_n$ que q divise, on a donc $\left(\frac{u}{q}\right) = -1$ et $h = p-2-k$. On a $\lambda_h \in \mathbb{F}_q$, on prend $\lambda \in \mathbb{Z}$ tel que la classe de λ modulo q soit λ_h et on considère la suite de Lucas-Lehmer $(v_n)_n$ vérifiant $v_0 = \lambda$. On a alors :

$$\begin{array}{lcl}
\overline{v_0} & = & \lambda_h \\
\overline{v_1} & = & \overline{v_0}^2 - 2 = \lambda_h^2 - 2 = \lambda_{h-1} \\
\overline{v_2} & = & \overline{v_1}^2 - 2 = \lambda_{h-1}^2 - 2 = \lambda_{h-2} \\
 & \vdots & \\
\overline{v_h} & = & \overline{v_{h-1}}^2 - 2 = \lambda_1^2 - 2 = \lambda_0 = \overline{u_0} \\
\overline{v_{h+1}} & = & \overline{v_h}^2 - 2 = \overline{u_0}^2 - 2 = \overline{u_1} \\
 & \vdots &
\end{array}$$

3/ En reprenant les notations du théorème précédent, on voit que

$$q|u_{p-2} \Longleftrightarrow \left(\frac{u}{q}\right) = -1 \ et \ h = 0 \Longleftrightarrow \left(\frac{u_0-2}{q}\right) = 1 \ et \ \left(\frac{u_0+2}{q}\right) = -1$$

3.— Recherche de bonnes valeurs initiales.

3.1.— Courbes associées à la suite de Lucas-Lehmer. On considère les deux

ensembles suivants :

$$A = \left\{ \lambda \in \mathbb{N} \text{ sans facteur carré } / \left(\frac{\lambda}{q}\right) = -1 \text{ pour tout } q \text{ premier de Mersenne assez grand} \right\}$$

$$B = \left\{ \lambda \in \mathbb{N} \text{ sans facteur carré } / \left(\frac{\lambda}{q}\right) = 1 \text{ pour tout } q \text{ premier de Mersenne assez grand} \right\}$$

et la famille de courbes $\mathcal{F}$ composée des courbes $\mathcal{C}_{a,b}$ d'équations :

$$aX^2 - bY^2 = 4$$

avec $a \in A$ et $b \in B$.

Proposition 6.— *Soit $\mathcal{C}_{a,b} \in \mathcal{F}$ et (x, y) un point entier de la courbe $\mathcal{C}_{a,b}$. L'entier $u_0 = ax^2 - 2 = by^2 + 2$ est une bonne valeur initiale de la suite de Lucas-Lehmer. Réciproquement, si u_0 est une bonne valeur initiale de la suite de Lucas-Lehmer alors il existe une courbe $\mathcal{C}_{a,b}$ possédant un point entier (x, y) qui vérifie $u_0 = ax^2 - 2 = by^2 + 2$.*

Preuve : On a pour tout premier de Mersenne assez grand $\left(\frac{u_0-2}{q}\right) = \left(\frac{by^2}{q}\right) = \left(\frac{b}{q}\right) = 1$ et $\left(\frac{u_0+2}{q}\right) = \left(\frac{ax^2}{q}\right) = \left(\frac{a}{q}\right) = -1$. Le corollaire 5 assure alors le résultat.

Réciproquement, si u_0 est une bonne valeur initiale de la suite de Lucas-Lehmer, alors si x^2 désigne le plus grand carré divisant $u_0 + 2$ et y^2 le plus grand carré divisant $u_0 + 2$, le point (x, y) est un point entier de la courbe $\mathcal{C}_{a,b}$ avec $a = \frac{u_0+2}{x^2}$ et $b = \frac{u_0-2}{y^2}$.

Remarque.— 1) La correspondance entre bonnes valeurs initiales et points entiers sur les courbes $\mathcal{C}_{a,b}$ est en fait biunivoque (au signe de x et de y près). En effet, si une bonne valeur initiale u_0 provient d'un point entier (x, y) d'une courbe $\mathcal{C}_{a,b}$ et aussi d'un point entier (x', y') d'une courbe $\mathcal{C}_{a',b'}$, on a alors $u_0 + 2 = ax^2 = a'x'^2$. Comme a et a' sont sans facteur carré, on en déduit que $a = a'$ et $x = \pm x'$ et, de la même manière, que $b = b'$ et $y = \pm y'$.

2) Si une courbe $\mathcal{C}_{a,b} \in \mathcal{F}$ possède un point entier alors nécessairement $\text{pgcd}(a, b) = 1$ ou 2. De même en regardant les résidus quadratiques on constate que pour tout $p \neq 2$ premier, si $p|a$ (resp. $p|b$) alors $\left(\frac{b}{p}\right) = \left(\frac{-1}{p}\right)$ (resp. $\left(\frac{a}{p}\right) = 1$). Cette propriété possède en fait une réciproque partielle :

Proposition 7.— *Soit $\mathcal{C}_{a,b} \in \mathcal{F}$, avec $\text{pgcd}(a, b) = 1$ ou 2. Si pour tout $p \neq 2$ premier, on a*

$$p|a \ (resp.\ p|b) \Longrightarrow \left(\frac{b}{p}\right) = \left(\frac{-1}{p}\right) \ (resp.\ \left(\frac{a}{p}\right) = 1)$$

alors $\mathcal{C}_{a,b}$ possède un point $\mathbb{Q}$-rationnel

Preuve : La forme quadratique rationnelle $f = aX^2 - bY^2$ est de rang 2, donc le théorème de Hasse assure que f représente 4 sur $\mathbb{Q}$ si et seulement si f représente 4 sur $\mathbb{Q}_p$ pour tout premier p (y compris $p = +\infty$), sauf éventuellement pour un p. Il est clair que f représente 4 sur $\mathbb{R}$. Prenons un premier $p \neq 2$ et montrons que f

représente 4 sur $\mathbb{Q}_p$. On va utiliser dans la suite de la preuve le résultat suivant : *un élément $\alpha \in \mathbb{Z}_p$ est un carré si et seulement si $v_p(\alpha)$ est pair et $p^{-v_p(\alpha)}\alpha$ est un carré modulo p.* On considère alors trois cas :

1) $\underline{p \text{ ne divise pas } ab}$. L'équation $f(X,Y) = 4$ équivaut à $X^2 = \dfrac{4+bY^2}{a}$. Modulo p, il existe $y \in \mathbb{F}_p$ tel que $\dfrac{4+by^2}{a}$ soit un carré de $\mathbb{F}_p$. En effet, quand y varie l'élément $\dfrac{4+by^2}{a}$ prend exactement $(p+1)/2$ valeurs, comme c'est aussi le nombre de carrés dans $\mathbb{F}_p$ et $(p+1)/2 + (p+1)/2 = p+1 > p$ on en déduit bien l'existence de y. Deux cas se présentent alors :

1.1) Si $\dfrac{4+by^2}{a} \neq 0$, alors si y_0 désigne un relevé de y dans $\mathbb{Z}_p$, la valuation de $\dfrac{4+by_0^2}{a}$ est nulle et par suite il s'agit d'un carré dans $\mathbb{Z}_p$.

1.2) Si $\dfrac{4+by^2}{a} = 0$, alors $-4/b$ est un carré non nul dans $\mathbb{F}_p$. Comme c'est un élément de valuation nulle dans $\mathbb{Z}_p$, c'est donc un carré de $\mathbb{Q}_p$. Ainsi $f(0, \sqrt{-4/b}) = 4$.

2) $\underline{p \text{ divise } a}$ (et donc p ne divise pas b). Comme $-4/b$ est un carré non nul dans $\mathbb{F}_p$ et que c'est un élément de valuation nulle dans $\mathbb{Z}_p$, c'est donc un carré de $\mathbb{Q}_p$. Ainsi $f(0, \sqrt{-4/b}) = 4$.

3) $\underline{p \text{ divise } b}$ (et donc p ne divise pas a). Comme $4/a$ est un carré non nul dans $\mathbb{F}_p$ et que c'est un élément de valuation nulle dans $\mathbb{Z}_p$, c'est donc un carré de $\mathbb{Q}_p$. Ainsi $f(\sqrt{4/a}, 0) = 4$.

Ainsi, pour la recherche de points entiers sur une courbe $\mathcal{C}_{a,b}$, la condition nécessaire

$$\text{(C) } \text{pgcd}(a,b) = 1, 2 \text{ et } \forall p \neq 2,\ p|a \Longrightarrow \left(\frac{b}{p}\right) = \left(\frac{-1}{p}\right) \text{ et } \forall p \neq 2,\ p|b \Longrightarrow \left(\frac{a}{p}\right) = 1$$

est "presque" suffisante. Elle va donc permettre d'éliminer "assez efficacement" des courbes $\mathcal{C}_{a,b}$ pour la recherche de bonnes valeurs initiales.

3.2.— Application à l'explicitation de familles infinies de bonne valeurs initiales. On cherche, dans cette partie, à donner explicitement des bonnes valeurs initiales de la suite de Lucas-Lehmer en utilisant la proposition 6. Pour cela on procède par étapes.

Etape I : On cherche des entiers dans A et B. Par exemple,

• Pour tout $p \geq 3$ on a $2^p \equiv 1 \bmod(q)$ et donc $2^{\frac{p+1}{2}}$ est une racine carrée de 2 modulo q. Donc $\left(\dfrac{2}{q}\right) = 1$ et ainsi $2 \in B$.

• La loi de réciprocité quadratique de Gauss assure que pour tout $p \geq 3$,

$$\left(\frac{3}{q}\right) = (-1)^{\frac{3-1}{2}\frac{q-1}{2}} \left(\frac{q}{3}\right) = (-1)^{2^{p-1}-1} \left(\frac{q}{3}\right) = -\left(\frac{q}{3}\right)$$

Comme $2 \equiv -1 \bmod(3)$, on a $q = 2^p - 1 \equiv -2 \equiv 1 \bmod(3)$ et donc $\left(\dfrac{3}{q}\right) = -1$. Ainsi $3 \in A$.

De manière plus générale, prenons en premier l, notons α_l l'ordre de 2 dans $\mathbb{F}_l^*$, et considérons (pour p grand) la division euclidienne $p = \alpha_l g + k$. On a alors

$$\left(\frac{l}{q}\right) = (-1)^{\frac{l-1}{2}\frac{2^p-2}{2}} \left(\frac{q}{l}\right) = (-1)^{\frac{l-1}{2}} \left(\frac{2^k-1}{l}\right)$$

et ainsi, quand p varie le symbole $\left(\frac{2^p-1}{l}\right)$ est égal, au facteur $(-1)^{\frac{l-1}{2}}$ près, à $\left(\frac{2^k-1}{l}\right)$ pour un certain entier $k < \alpha_l$, premier à α_l (puisque p est premier). En d'autres termes, le symbole $\left(\frac{2^p-1}{l}\right)$ ne dépend que de la congruence modulo α_l de p. Par exemple

• Pour $l = 5$ on a $\alpha_5 = 4$ et on trouve pour tout q

$$\left(\frac{5}{q}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \bmod(4) \\ -1 & \text{si } p \equiv 3 \bmod(4) \end{cases}$$

• Pour $l = 7$ on a $\alpha_7 = 3$ et on trouve pour tout $q \neq 7$

$$\left(\frac{7}{q}\right) = \begin{cases} 1 & \text{si } p \equiv 2 \bmod(3) \\ -1 & \text{si } p \equiv 1 \bmod(3) \end{cases} = \begin{cases} 1 & \text{si } p \equiv 5, 11 \bmod(12) \\ -1 & \text{si } p \equiv 1, 7 \bmod(12) \end{cases}$$

• Pour $l = 13$ on a $\alpha_{13} = 12$ et on trouve pour tout $q \neq 3, 7$

$$\left(\frac{13}{q}\right) = \begin{cases} 1 & \text{si } p \equiv 1, 7 \bmod(12) \\ -1 & \text{si } p \equiv 5, 11 \bmod(12) \end{cases}$$

On remarque que, sur ces deux derniers exemples, les valeurs en fonction des congruences sont opposées, de sorte que pour tout $q \neq 3, 7$ on a

$$\left(\frac{7.13}{q}\right) = -1$$

et ainsi $91 \in A$.

On peut décrire un algorithme qui permet de calculer (assez efficacement) des valeurs de A et de B :

• On se fixe un entier n et $l_1 < \cdots < l_n$ des nombres premiers.

• On calcule $\alpha_{l_1}, \cdots, \alpha_{l_n}$ et on pose $\alpha = \text{ppcm}(\alpha_{l_1}, \cdots, \alpha_{l_n})$.

• Pour tout $k \leq \alpha$ premier à α on calcule

$$\left(\frac{2^k-1}{l_1}\right).\cdots.\left(\frac{2^k-1}{l_n}\right)$$

et si ce produit est toujours égal à 1 alors l'entier $l_1.\cdots.l_n$ est élément de A ou de B (le choix de l'ensemble se fait en calculant $(-1)^{\frac{l_1-1}{2}}.\cdots.(-1)^{\frac{l_1-1}{2}}$)

On calcule ensuite tous les produits possibles de ces éléments (en retirant à chaque fois les facteurs carrés). On détermine alors ceux qui appartiennent à A et ceux qui appartiennent à B.

Remarque 8.— Puisque le test a lieu sur tous les entiers k premier à α, il est clair que ce test ne détermine pas *a priori* toutes les valeurs de A et B. Toutefois, si l'on fait l'hypothèse suivante :

(H) Pour tout entier $n \geq 2$ et tout entier k premier à n, il existe une infinité de premiers $p \equiv k \bmod(n)$ tel que $2^p - 1$ soit premier.

alors le test caractérise tous les éléments de A et B. Rappelons qu'on ne sait toujours pas si les nombres premiers de Mersenne sont ou non en nombre infini. L'hypothèse (H) peut donc paraitre assez audacieuse.

Etape II : On obtient donc des courbes associées aux valeurs trouvées. On élimine alors les courbes $\mathcal{C}_{a,b}$ qui ne vérifie pas la condition (C) et on cherche des points entiers sur ces courbes.

Remarque 9.— Soient a, b obtenus par cet algorithme et u_0 une bonne première valeur initiale provenant d'un point entier de la courbe $\mathcal{C}_{a,b}$. Le test de Lucas-Lehmer pour la valeur initiale u_0 est nécessaire suffisant pour le nombre premier de Mersenne q dès que q ne divise ni a ni b.

Application : Nous avons appliqué l'algorithme pour $n = 1, 2, 3, 4$ et $l_n < 1000$ (Calculs sous Maxima sur un PC de configuration standard). Nous avons trouvé les valeurs suivantes :

{2, 3, 13.7, 13.7.3, 41.31.5, 109.37.19, 241.7.5, 241.13.5, 41.31.5.3, 109.37.19.3, 241.7.5.3, 241.13.5.3, 241.41.31.7, 241.41.31.13, 331.31.11.7, 331.31.13.11, 331.241.41.11}

S'en est suivie l'obtention de 68 valeurs pour chacun des ensembles A et B. Après élimination des courbes qui ne satisfaisaient pas la condition (C), il n'en resta que 4. Ce sont les courbes :

$$\begin{array}{ll} (E_1): & 6x^2 - 2y^2 = 4 \\ (E_2): & 3x^2 - 2y^2 = 4 \\ (E_3): & \lambda x^2 - 2y^2 = 4 \\ (E_4): & 2\lambda x^2 - 2y^2 = 4 \end{array}$$

avec $\lambda = 107930163$.

Les paragraphes suivants s'intéressent à la recherche exhaustive des points entiers de (E_1) et (E_2).

3.3.— Résolution de (E_1). L'équation (E_1) équivaut à $x^2 - 3y^2 = -2$. Ceci nous conduit à considérer l'anneau $A = \mathbb{Z}[\sqrt{3}]$ et sa norme $N(x + y\sqrt{3}) = x^2 - 3y^2$. Cet anneau est euclidien pour le stathme $|N(.)|$. Les solutions de (E_1) correspondent aux éléments de A de norme -2. Nous allons montrer que les éléments de norme -2 de A sont associés.

L'élément $v = 1+\sqrt{3}$ est visiblement de norme -2. Soit u un autre élément de A de norme -2 et $u = qv+r$ la division euclidienne de u par v. On a $|N(r)| < 2$, c'est-à-dire $|N(r)| = 0$ ou 1. Si $N(r) = 0$ alors $r = 0$ et v divise u, mais alors $|N(q)| = 1$ et donc u et v sont associés. Supposons que $N(r) = 1$, r est donc inversible dans A et on a alors $r^{-1}u = r^{-1}vq + 1$. En posant formellement $r^{-1}q = x + y\sqrt{3}$ on en déduit que $N((1+\sqrt{3})(x+y\sqrt{3})+1) = -2$ ce qui équivaut à $(x+3y+1)^2-3(x+y)^2 = -2$, c'est-à-dire après simplification

$$-2x^2 + 6y^2 + 2x + 6y = -3$$

Cette dernière équation n'a pas de solution (sinon modulo 2 on aurait $0 = -3$).

On en déduit que tous les éléments de norme -2 sont associés à $1 + \sqrt{3}$ et par suite la résolution de (E) est ramenée à la recherche des unités de A ce qui équivaut à trouver les solutions de l'équation de Pell-Fermat $x^2 - 3y^2 = 1$ (en réduisant modulo 3 on voit que $N(u) = -1$ n'a pas de solution dans A). L'unité primitive (la plus petite > 1) de A est $u = 2 + \sqrt{3}$. On sait alors que l'ensemble des unités de A est $\{\pm u^n / \ n \in \mathbb{Z}\}$. Pour notre problème, on peut se limiter à considérer l'ensemble $\{u^n / \ n \in \mathbb{N}\}$.

Ainsi les solutions de (E) sont tous les couples $(\pm y_n, \pm x_n)$ où les deux suites $(x_n)_n$ et $(y_n)_n$ sont définies par la relation $(x_n + y_n\sqrt{3}) = (1+\sqrt{3})(2+\sqrt{3})^n$. On obtient par récurrence que pour tout $n \geq 1$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Le polynôme caractéristique de la matrice vaut $X^2 - 4X + 1$, la suite $(x_n)_n$ est donc caractérisée par $x_0 = 1, x_1 = 5$ et pour tout $n \geq 0$

$$x_{n+2} = 4x_{n+1} - x_n$$

En prenant $u_0 = 2x_n^2 + 2$ on obtient donc une bonne valeur initiale de la suite de Lucas-Lehmer pour $p \geq 3$ (en vertu de la remarque 9). Voici les 30 premières valeurs obtenues :

n	x_n	u_0
0	1	4
1	5	52
2	19	724
3	71	10 084
4	265	140 452
5	989	1 956 244
6	3 691	27 246 964
7	13 775	379 501 252
8	51 409	5 285 770 564
9	191 861	73 621 286 644
10	716 035	1 025 412 242 452
11	2 672 279	14 282 150 107 684
12	9 973 081	198 924 689 265 124
13	37 220 045	2 770 663 499 604 052
14	138 907 099	38 590 364 305 191 604
15	518 408 351	537 494 436 773 078 404
16	1 934 726 305	7 486 331 750 517 906 052
17	7 220 496 869	104 271 150 070 477 606 324
18	26 947 261 171	1 452 309 769 236 168 582 484
19	100 568 547 815	20 228 065 619 235 882 548 452
20	375 326 930 089	281 740 608 900 066 187 095 844
21	1 400 739 172 541	3 924 140 458 981 690 736 793 364
22	5 227 629 760 075	54 656 225 816 843 604 128 011 252
23	19 509 779 867 759	761 263 020 976 828 767 055 364 164
24	72 811 489 710 961	10 603 026 067 858 759 134 647 087 044
25	271 736 178 976 085	147 681 101 929 045 799 118 003 854 452
26	1 014 133 226 193 379	2 056 932 400 938 782 428 517 406 875 284
27	3 784 796 725 797 431	28 649 372 511 213 908 200 125 692 399 524
28	14 125 053 676 996 345	399 034 282 756 055 932 373 242 286 718 052
29	52 715 417 982 187 949	5 557 830 586 073 569 145 025 266 321 653 204

3.4.— Résolution de (E_2). Commencons par expliquer comment, de manière générale, trouver toutes les solutions entières d'une équation (E) $\lambda a^2 - 2b^2 = 4$ avec λ impair (une fois qu'on en connait une).

Si $\lambda a^2 - 2b^2 = 4$ alors $2|a^2$ et par suite $4|a^2$. Ainsi $2|b^2$ et donc la resolution de (E) équivaut alors à celle de l'équation $2a^2 - \lambda b^2 = -1$, où mieux à celle de l'équation $(2a)^2 - 2\lambda b^2 = -2$. On se place dans l'anneau $A = \mathbb{Z}[2\lambda]$ muni de la norme $N(x + y\sqrt{2\lambda}) = x^2 - 2\lambda y^2$ dont on cherche les éléments de norme -2. Si $N(x+y\sqrt{2\lambda}) = -2$ alors x est pair, ce qui montre que la résolution de notre équation revient exactement à trouver les éléments de norme -2 de A. Malheureusement A n'est pas un anneau euclidien, mais on peut toutefois remarquer que si $2x + y\sqrt{2\lambda}$ et $2x^{'} + y^{'}\sqrt{2\lambda}$ sont deux éléments de norme -2 alors on a

$$\frac{2x + y\sqrt{2\lambda}}{2x^{'} + y^{'}\sqrt{2\lambda}} = \frac{(2x + y\sqrt{2\lambda})(2x^{'} - y^{'}\sqrt{2\lambda})}{-2} = (-2xx^{'} + \lambda yy^{'}) + (xy^{'} - x^{'}y)\sqrt{2\lambda} \in A$$

Donc les éléments de norme -2 sont tous associés. La résolution se ramène donc à la recherche des unités de A, ce qui revient à résoudre l'équation de Pell-Fermat $x^2 - 2\lambda y^2 = \pm 1$.

Dans le cas $\lambda = 3$, on a $A = \mathbb{Z}[\sqrt{6}]$ et l'élément $2 + \sqrt{6}$ est visiblement de norme -2. Pour la recherche des unités de A, on constate (en regardant modulo 3) que l'équation de Pell-Fermat $x^2 - 6y^2 = -1$ n'a pas de solution. On cherche donc les solutions de $x^2 - 2\lambda y^2 = 1$: l'unité fondamentale de $\mathbb{Z}[\sqrt{6}]$ est $u = 5 + 2\sqrt{6}$. Les solutions dans $\mathbb{N}$ de $x^2 - 6y^2 = -2$ sont donc les couples (x_n, y_n) avec $(x_0, y_0) = (2, 1)$ et pour tout $n \geq 0$

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

Le polynôme caractéristique de la matrice vaut $X^2 - 10X + 1$, la suite $(y_n)_n$ est donc caractérisée par $y_0 = 1, y_1 = 9$ et pour tout $n \geq 0$

$$y_{n+2} = 10y_{n+1} - y_n$$

En prenant $u_0 = 12y_n^2 - 2$ on obtient donc une bonne valeur initiale de la suite de Lucas-Lehmer pour $p \geq 3$ (en vertu de la remarque 9). Voici les 20 premières valeurs obtenues :

n	y_n	u_0
0	1	10
1	9	970
2	89	95 050
3	881	9 313 930
4	8 721	912 670 090
5	86 329	89 432 354 890
6	854 569	8 763 458 109 130
7	8 459 361	858 729 462 339 850
8	83 739 041	84 146 723 851 196 170
9	828 931 049	8 245 520 207 954 884 810
10	8 205 571 449	807 976 833 655 727 515 210
11	81 226 783 441	79 173 484 178 053 341 605 770
12	804 062 262 961	7 758 193 472 615 571 749 850 250
13	7 959 395 846 169	760 223 786 832 147 978 143 718 730
14	78 789 896 198 729	74 494 172 916 077 886 286 334 585 290
15	779 939 566 141 121	7 299 668 721 988 800 708 082 645 639 690
16	7 720 605 765 212 481	715 293 040 581 986 391 505 812 938 104 330
17	76 426 118 085 983 689	70 091 418 308 312 677 566 861 585 288 584 650
18	756 540 575 094 624 409	6 868 243 701 174 060 415 160 929 545 343 191 370
19	7 488 979 632 860 260 401	673 017 791 296 749 608 008 204 233 858 344 169 610

Bibliographie

[B] J. W. Bruce, *A Really Trivial Proof of the Lucas-Lehmer Test*, Am. Math. Mon. 100, No. 4, 370-371 (1993).

[R] M. I. Rosen *A proof of the Lucas-Lehmer test.*, Am. Math. Mon. 95, No. 9, 855-856 (1988).

Bruno Deschamps
Département de Mathématiques — Université du Maine
Avenue Olivier Messiaen, 72085 Le Mans cedex 9 - France
E-mail : Bruno.Deschamps@univ-lemans.fr