Collect. Math. **46**, 1–2 (1995), 195–216

Suite de LUCAS et Cryptographie

André Warusfel

Inspection Générale de Mathématiques,

107 Rue de Grenelle, 75 007 Paris

Dédié à la mémoire de Paul Dubreil

Abstract

The Lucas sequence is a sort of generalization of ordinary powers, with properties similar in respect of Fermat's theorem. This sequence can be used for cryptographic procedures, in the sense that $v_{n+m} = v_n \circ v_m$ is similar to the usual property $\alpha^{n+m} = \alpha^n \alpha^m$.

I. Définition et premières propriétés

I.1) Définition de la suite v de Lucas.

Soit $\mathcal{A}$ un anneau (unitaire) commutatif et $p \in \mathcal{A}$. On définit la suite de Lucas $v : \mathbb{N} \to \mathcal{A}$ par les égalités:

$$\boxed{v_0 = 2, \qquad v_1 = p, \qquad v_{n+2} = p\, v_{n+1} - v_n}$$

On pose $D = p^2 - 4 \in \mathcal{A}$ (*discriminant* de la suite v).

I.2) Premières remarques.

a) Il est immédiat de prolonger l'ensemble de définition de v de $\mathbb{N}$ à $\mathbb{Z}$, en posant, pour tout $n \in \mathbb{Z}$:

$$v_{-n} = v_n.$$

b) On pourra trouver intérêt à noter $v_n(p)$, expression polynômiale à coefficients entiers en p, de terme dominant p^n pour $n > 0$, en lieu et place de v_n.

De cette notation résulte aussitôt l'existence d'une suite de fonctions polynômiales, indexées par $\mathbb{N}$ (voire $\mathbb{Z}$), naturellement notées $v_n : \mathcal{A} \to \mathcal{A}$, d'expression explicite:

$$v_n(p) = \sum_k (-1)^k \frac{n}{n-k} C_{n-k}^k \, p^{n-2k}$$

(la sommation porte sur les entiers naturels tels que $2k \leq n$).

c) Si p et p' sont congrus modulo $N \in \mathcal{A}$ (c'est–à–dire si $p' - p = k\,N$ avec $k \in \mathbb{Z}$), il en est de même de $v_n(p)$ et de $v_n(p')$ pour tout n.

d) La définition initiale d'Edouard Lucas en 1876 consistait à poser $v_{n+2} = p\,v_{n+1} - q\,v_n$. Il considérait également la suite jumelle u définie par la même relation de récurrence et les valeurs initiales $u_0 = 0$ et $u_1 = 1$ (cf. **II.3**).

e) Les polynômes v_n portent également le nom de "polynômes de DICKSON", étudiés en 1896, dans la thèse de ce dernier, sous la forme $D_n(X, a) = (\sqrt{a})^n\, v_n(X/\sqrt{a}) \in \mathbb{F}_q[X]$ [d'où $v_n(p) = D_n(p, 1)$].

f) Si $\mathcal{A} = \mathbb{C}$ et si $(a, b) = (e^{i\theta}, e^{-i\theta})$ sont tels que $p = a + b = 2\cos\theta$ (et $ab = 1$), il vient aussitôt l'égalité de TCHEBITCHEFF:

$$v_n(p) = a^n + b^n = 2\cos\left[n \operatorname{Arc}\cos\frac{p}{2}\right] = 2\cos n\theta.$$

I.3) Plongement canonique de l'anneau $\mathcal{A}$.

Définissons une injection canonique de $\mathcal{A}$ dans l'ensemble $\mathcal{A}^2$, muni d'une structure d'anneau commutatif isomorphe à un sous–anneau de $\mathcal{M}_2(\mathcal{A})$, par les opérations:

$$x \mapsto (x, 0),$$

$$(x, y) + (x', y') = (x + x', y + y'), \quad (x, y)\,(x', y') = (xx' - yy', xy' + x'y + p\,yy'),$$

$$(x, y) \mapsto xI + yA = \begin{pmatrix} x & -y \\ y & x + py \end{pmatrix}.$$

On a aussitôt $A^2 = p\,A - I$ et, pour $B = A^{-1} = p\,I - A$, $B^2 = p\,B - I$ d'où l'égalité fondamentale:

$$v_n(p) \mapsto v_n(p)\,I = A^n + B^n.$$

Pour tout polynôme $P \in \mathbb{Z}[X]$, la matrice $P(A)+P(B)$ est scalaire, c'est–à–dire de la forme $k\,I$ avec $k \in \mathcal{A}$.

I.4) Premières propriétés de la suite v de Lucas.

a) Soit $0 \leq m \leq n$; il vient:

$$v_{n+m} = v_n\, v_m - v_{n-m}$$

ce qui fournit les égalités:

$$v_{2n-1} = v_n\, v_{n-1} - p\,, \quad v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}\, v_n - p\,.$$

b) Signalons aussi l'égalité:

$$(v_n - p\,)^2 = (v_{n-1} - 2)\,(v_{n+1} - 2)$$

ainsi surtout que la relation fondamentale:

$$\boxed{v_{nm} = v_n \circ v_m}$$

soit encore, pour tout triplet $(n, m, p\,)$, $v_{nm}(p\,) = v_n\big(v_m(p\,)\big)$, qui traduit l'identité immédiate $A^{nm} + B^{nm} = (A^m)^n + (B^m)^n$.

II.— Calcul de la suite v de Lucas

II.1) Un algorithme de calcul de $v_n(p\,)$.

Les relations démontrées en **I.4)** a) conduisent évidemment à un algorithme de calcul de $v_n(p\,)$, de complexité $O\,(\log n)$, explicité dans le cas $\mathcal{A} = \mathbb{Z}$ par la pseudo–procédure Pascal ci–dessous.

Une variante de cette procédure conduit au calcul, toujours en $O\,(\log n)$, du reste modulo N de $v_n(p\,)$, donc de $v_n(p\,)$ dans le cas $\mathcal{A} = \mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$.

II.2) Une procédure Pascal pour $v_n(p)$.

La procédure ci–dessous, valable à partir de $n = 0$, est en $O(\log n)$:

```
VAR d, n, p, t, v : INTEGER;
READ(n);
d ← 1;
WHILE d <= n DO d ← 2 * d;
READ(p);
(v, t) ← (2, p);
WHILE d > 1 DO
BEGIN
  d ← d DIV 2;
  IF ODD(n DIV d)
    THEN (v, t) ← (t * v − p, t^2 − 2)
    ELSE (v, t) ← (v^2 − 2, t * v − p)
END;
WRITE(v);
```

En fin d'exécution, après 2ℓ boucles, où $\ell = 1 + [\log_2 n]$, v a pour valeur $v_n(p)$. Cette procédure peut facilement s'étendre à des calculs modulo N.

Pour vérifier cette procédure, on exhibera un *invariant de boucle*, comme le triplet $(m - n \text{ DIV } d,\ v_m - v,\ v_{m+1} - t)$, constamment égal à $(0, 0, 0)$.

II.3) Définition de la suite u de Lucas.

Nous introduisons ici, à côté de v, la suite jumelle u définie plus haut par $u_0 = 0$ et $u_1 = 1$.

Cette dernière suite est liée à v par de très nombreuses relations. En particulier, on peut vérifier facilement les égalités suivantes :

$$u_{2n}(p) = \sum_{m=1}^{n} v_{2m-1}(p), \qquad u_{2n+1}(p) = 1 + \sum_{m=1}^{n} v_{2m}(p),$$

provenant de l'injection canonique :

$$u_n(p) \mapsto u_n(p)\, I = \sum_{m=1}^{n} A^{n-m} B^{m-1}$$

qui implique l'égalité fondamentale reliant u à la seconde famille de polynômes de Tchebitcheff:

$$u_n(p)\,(A-B) = A^n - B^n.$$

(Si $\mathcal{A} = \mathbb{C}$ et $p = 2\cos\theta$, on a $u_n(p) = \dfrac{\sin n\theta}{\sin\theta}$.)

En sens inverse, on obtient v_n à partir de u_n par les relations immédiates:

$$v_n(p) = u_{n+1}(p) - u_{n-1}(p) = p\,u_n(p) - 2\,u_{n-1}(p) = 2\,u_{n+1}(p) - p\,u_n(p),$$

éventuellement étendues à $\mathbb{Z}$, si l'on pose $u_{-n}(p) = -u_n(p)$. Notons aussi, lorsque cela a un sens, l'égalité $v_n = u_{2n}/u_n$.

Entre u_n et v_n existent des liens formels très importants. Notant $\delta = A - B$, il vient $\delta^2 = D\,I$ et:

$$u_n\,\delta + v_n\,I = 2\,A^n,$$

$$2^{n-1}(u_n\,\delta + v_n\,I) = (\delta + p\,I)^n.$$

La dernière de ces égalités permet, à cause de l'indépendance de I et de $\delta = \begin{pmatrix} -p & -2 \\ 2 & p \end{pmatrix}$ [vraie si 2 est inversible dans $\mathcal{A}$], d'obtenir de nombreuses propriétés de $u_n(p)$ et de $v_n(p)$. Elles restent cependant valides pour tout anneau comme on peut le voir par récurrence. On dispose, par exemple, des identités fondamentales:

$$2\,u_{n+1} = v_n + p\,u_n, \qquad 2\,v_{n+1} = p\,v_n + D\,u_n$$

ainsi que:

$$v_n^2 - D\,u_n^2 = 4.$$

Pour que le couple (u, v) engendre le $\mathcal{A}$–module des suites solutions de l'équation fonctionnelle $x_{n+2} = p\,x_{n+1} - x_n$, il faut et il suffit que 2 soit inversible dans $\mathcal{A}$. Par exemple $v_n = u_{n+1} - u_{n-1} = p\,u_n - 2\,u_{n-1}$ implique $v = p\,u$ si $\mathcal{A}$ est de caractéristique 2. Mais dans tous les cas l'on dispose d'une base (u, w) en posant pour tout n (éventuellement dans $\mathbb{Z}$):

$$w_n = u_{n-1},$$

puisqu'alors $x = x_1\,u - x_0\,w$.

Il existe d'autres relations entre u et v, comme des formes équivalentes de deux égalités jumelles:

$$2\,v_{n+m} = v_n v_m + D\,u_n u_m, \qquad 2\,v_{n-m} = v_n v_m - D\,u_n u_m$$
$$2\,u_{n+m} = u_n v_m + v_n u_m, \qquad 2\,u_{n-m} = u_n v_m - v_n u_m,$$

utilisables pour le calcul de $v_n(p)$ et $u_n(p)$, dont nous avons déjà signalé des cas particuliers pour $m = 1$ ou $m = n$.

La suite u permet d'écrire simplement A^n et B^n:

$$A^n = u_n\,A - u_{n-1}\,I = \begin{pmatrix} -u_{n-1} & -u_n \\ u_n & u_{n+1} \end{pmatrix}$$
$$B^n = u_n\,B - u_{n-1}\,I = \begin{pmatrix} u_{n+1} & u_n \\ -u_n & -u_{n-1} \end{pmatrix}.$$

On en déduit aussitôt les égalités suivantes, permettant le calcul de $u_n(p)$ sans recourir à $v_n(p)$:

$$u_{n+m} = p\,u_n u_m - u_n u_{m-1} - u_m u_{n-1}, \qquad u_{n+m-1} = u_n u_m - u_{n-1} u_{m-1}.$$

Voici une expression explicite de u:

$$u_{n+1}(p) = \sum_k (-1)^k\,C_{n-k}^k\,p^{n-2k}$$

(la sommation porte sur les entiers naturels tels que $2k \leq n$).

II.4) Un algorithme de calcul du couple $\big(u_n(p),\,v_n(p)\big)$.

Si l'on peut diviser par 2 dans l'anneau $\mathcal{A}$, un premier algorithme, également en $O(\log n)$, est basé sur les formules:

$$u_{2n} = u_n\,v_n = \alpha\,\beta, \qquad v_{2n} = v_n^2 - 2 = \beta^2 - 2,$$

$$u_{2n+1} = \frac{1}{2}\,[v_{2n} + p\,u_{2n}] = \frac{1}{2}\,\beta\,[p\,\alpha + \beta] - 1,$$

$$v_{2n+1} = \frac{1}{2}\,[p\,v_{2n} + D\,u_{2n}] = \frac{1}{2}\,\beta\,[D\,\alpha + p\,\beta] - p$$

où $\alpha = u_n(p)$ et $\beta = v_n(p)$. Il permet de calculer, selon le cas, l'un des deux couples $(u_{2n},\,v_{2n})$ et $(u_{2n+1},\,v_{2n+1})$ à partir de $(\alpha,\,\beta)$.

II.5) Une procédure Pascal pour $\big(u_n(p),\,v_n(p)\big)$.

La pseudo–procédure en $O(\log n)$ ci–dessous, due à R. Nöbauer, valable à partir de $n = 0$ et basée sur une technique analogue à l'"exponentiation rapide", semble

plus efficace pour obtenir $\big(u_n(p)\,,\,v_n(p)\big)$, ou même le seul $v_n(p)$ à partir de $u_n(p)$ et $u_{n-1}(p)$:

```
VAR n, p, r, s, u, v, w : INTEGER;
(r, s) ← (1, 0); (u, w) ← (0, −1);
READ(n); READ(p);
WHILE n > 0 DO
BEGIN
  IF ODD(n) THEN (u, w) ← (p ∗ r ∗ u − r ∗ w − s ∗ u, r ∗ u − s ∗ w);
  n ← n DIV 2;
  (r, s) ← (r ∗ (p ∗ r − 2 ∗ s), r^2 − s^2)
END;
v ← p ∗ u − 2 ∗ w;
WRITE(u); WRITE(v);
```

Pour vérifier cette procédure, il suffit d'exhiber un *invariant de boucle*, comme la matrice $(uA - wI)\,(rA - sI)^m$, constamment égale à A^n.

III.— Une divisibilité remarquable dans $\mathbb{Z}[X]$

Dans cette partie $\mathcal{A} = \mathbb{Z}$

Théorème. *[dû pour l'essentiel à* **Lucas***: cf. sa note aux CRAS de 1877].*

Soit N un entier strictement positif. Il existe alors un algorithme explicite, basé sur la décomposition de N en facteurs premiers, donnant un entier $r > 0$ tel que, pour tout $(h, p) \in \mathbb{N} \times \mathbb{Z}$ tel que $D = p^2 - 4$ soit premier avec N, il existe $(Q, H) \in \mathbb{Z}[X]^2$, avec H de degré au plus 1, tel que:

$$X^{hr} - 1 = (X^2 - p\,X + 1)\,Q(X) + N\,H(X) = T(X)\,Q(X) + N\,H(X)$$

III.1) Premières remarques.

Puisque $X^r - 1$ divise $X^{hr} - 1$ dans $\mathbb{Z}[X]$, il suffit de prouver le théorème pour $h = 1$.

Notons que Q est le quotient de $X^{hr} - 1$ par T. Si le théorème est connu pour deux entiers N' et N'' premiers entre eux, on peut donc le prouver pour leur produit N, puisque le $PPCM$ r de r' et r'' est tel que $X^r - 1 - T(X)\,Q(X)$ est un polynôme entier, multiple de N' et de N'' et donc de N.

Puisque l'on peut remplacer H par son reste modulo T, on voit que la condition sur le degré de H est sans importance.

Les remarques précédentes montrent donc qu'il suffit de démontrer le théorème sans référence au degré de H, pour $h = 1$ et $N = \pi^n$ (nombre dit "primaire") avec π premier.

Si l'on note $\bar{x} \in \mathbb{Z}_N$ la classe modulo N d'un entier $x \in \mathbb{Z}$, on en déduit que le trinôme $\bar{T}(X) = X^2 - \bar{p}\,X + \bar{1}$ divise $X^{hs} - \bar{1}$ dans $\mathbb{Z}_N[X]$.

III.2) Cas particulier $N = 2$.

Ici "2 est premier avec D" signifie simplement "p est impair". L'entier $r = 3$ convient, puisque, pour tout entier impair p, on a:

$$X^3 - 1 = (X + p)\,(X^2 - p\,X + 1) + (p + 1)\,[(p - 1)\,X - 1]$$

avec $p + 1$ pair.

III.3) Cas particulier $N = \pi$ premier impair.

Proposition

Soient p un entier, $D = p^2 - 4$, π un nombre premier impair ne divisant pas D et $r = \pi - 1$ si D est un carré dans $\mathbb{F}_\pi$, $r = \pi + 1$ sinon, ce que l'on peut résumer à l'aide de l'indicateur de LEGENDRE *par la formule:*

$$r = \pi - \left(\frac{D}{\pi}\right).$$

Alors pour tout entier $h \in \mathbb{N}$ il existe un couple $(Q, H) \in \mathbb{Z}[X]^2$ tel que:

$$X^{hr} - 1 = (X^2 - p\,X + 1)\,Q(X) + \pi\,H(X).$$

La division euclidienne dans $\mathbb{Z}[X]$ nous donne:

$$X^r - 1 = (X^2 - p\,X + 1)\,Q(X) \;+\; k\,X + \ell.$$

Montrons tout d'abord que $\bar{D} = \bar{p}^2 - \bar{4}$ est un carré d^2 dans $\mathbb{F}_\pi$ si, et seulement si, $X^2 - \bar{p}\,X + \bar{1}$ admet une racine a dans $\mathbb{F}_\pi$; en effet $a^2 - \bar{p}\,a + \bar{1} = \bar{0}$ implique $\bar{D} = (\bar{2}\,a - \bar{p})^2$ et, inversement, $\bar{2}^{-1}(\bar{p} + d)$ annule $X^2 - \bar{p}\,X + \bar{1}$.

Dans ce cas, $X^2 - \bar{p}\,X + \bar{1} = (X - a)\,(X - b)$ avec $b = a^{-1} = \bar{p} - a$; π ne divisant pas D, a et b sont distincts. Dans le corps fini $\mathbb{F}_\pi$ on a $a^r = a^{\pi - 1} = \bar{1} = b^r$; par suite:

$$\bar{k}\,a + \bar{\ell} = \bar{k}\,b + \bar{\ell} = \bar{0}$$

d'où $\bar{k}\,(b - a) = \bar{0}$, $\bar{k} = \bar{0}$ et enfin $\bar{\ell} = \bar{0}$ ce qui montre que $H(X) = (\pi^{-1}k)\,X + \pi^{-1}\ell$ convient.

Dans le cas contraire, $X^2 - \bar{p}\,X + \bar{1}$, irréductible dans $\mathbb{F}_\pi[X]$, ne se factorise en $(X - a)\,(X - b)$ que dans le sur–corps $\mathbb{F}_{\pi^2}$, isomorphe à $\mathbb{F}_\pi[X]/(X^2 - \bar{p}\,X + \bar{1})$. Posons $c = a^r = a^{\pi+1}$: on a $c^{\pi-1} = a^{\pi^2-1} = \bar{1}$, d'où $c \in \mathbb{F}_\pi$. Posons dans l'anneau $\mathbb{F}_\pi[X]$:

$$X^r - c = (X^2 - \bar{p}\,X + \bar{1})\,M(X) \,+\, u\,X + v.$$

De l'égalité $u\,a + v = \bar{0}$, on déduit aussitôt $u = v = \bar{0}$, puis $b^r = c$ et enfin (en caractéristique première π) :

$$\bar{p} = \bar{p}^\pi = (a + b)^\pi = a^\pi + b^\pi = (a^\pi + b^\pi)\,ab = a^r b + b^r a = c\,(b + a) = c\,\bar{p}.$$

Si $\bar{p} \neq \bar{0}$, on en déduit $c = \bar{1}$ et, comme ci–dessus, la congruence polynômiale annoncée. Sinon π divise p. S'il était de la forme $4\,n+1$, on disposerait des congruences modulo π:

$$D \equiv -4 \equiv 4\,(\pi - 1)! \equiv 4 \prod_{k=1}^{2n} k\,(\pi - k) \equiv (-1)^{2n} 4\,\big[(2\,n)!\big]^2 = [2\,(2\,n)!]^2$$

et $\bar{D}$ serait un carré dans $\mathbb{F}_\pi$; par suite π est du type $4n - 1$, d'où:

$$X^r - 1 = X^{\pi+1} - 1 = (X^2 + 1)\,Q(X) = (X^2 - p\,X + 1)\,Q(X) + \pi\,H(X).$$

III.4) Cas particulier $N = \pi^n$.

Pour tout premier π et tout entier p tel que π ne divise pas D, nous disposons donc désormais d'un entier $s = \pi \pm 1$ tel que, pour tout entier h, $X^{hs} - 1$ soit congru modulo π à un multiple du trinôme T. Cela constitue le cas particulier $n = 1$ de la proposition suivante:

Proposition

Soient p un entier, $D = p^2 - 4$ et π un nombre premier ne divisant pas D. Il existe alors un entier s de la forme $\pi \pm 1$ et $r = \pi^{n-1}s$ tels que, pour tout $(h, n) \in \mathbb{N} \times \mathbb{N}^*$, il existe un couple $(Q, H) \in \mathbb{Z}[X]^2$ tel que:

$$X^{hr} - 1 = X^{h\pi^{n-1}s} - 1 = (X^2 - p\,X + 1)\,Q(X) + \pi^n\,H(X).$$

Ici encore, il suffit de le prouver pour $h = 1$. La démonstration se fait alors par récurrence sur n. Posant $Y = X^r - 1 = X^{\pi^{n-1}s} - 1 = T\,Q + \pi^n H$, il vient aussitôt:

$$\begin{aligned} X^{\pi^n s} - 1 &= (Y+1)^\pi - 1 = Y^\pi + \pi\,Y\,L \\ &= (T\,Q + \pi^n H)^\pi + \pi\,(T\,Q + \pi^n H)\,L \\ &= T\,\hat{Q} + \pi^{n\pi} H^\pi + \pi^{n+1} H\,L \\ &= T\,\hat{Q} + \pi^{n+1}\hat{H} \end{aligned}$$

ce qui démontre le théorème dans le cas général.

III.5) Application à la suite de Lucas.

Si N est un entier premier avec D, on dispose de la congruence $v_n(p\,) \equiv v_\ell(p\,) \quad [N]$ dans $\mathbb{Z}$ pour tout indice n congru à ℓ modulo r.

L'injection canonique $v_n \mapsto A^n + B^n \in \mathcal{M}_2(\mathbb{Z})$ donne en effet $A^{hr} - I = N\,H(A)$ ainsi que $B^{hr} - I = N\,H(B)$, puis:

$$v_{hr+\ell} I = A^{hr+\ell} + B^{hr+\ell} = A^\ell + B^\ell + N\big(A^\ell H(A) + B^\ell H(B)\big) = [v_\ell(p\,) + kN]I.$$

III.6) Un cas particulier, fondamental en cryptographie.

Si N est le produit de deux nombres premiers impairs distincts π et ω, on dispose pour tout entier p tel que N soit premier avec D, de la congruence dans $\mathbb{Z}$:

$$v_{mr+\ell}(p\,) \equiv v_\ell(p\,) \quad [N]$$

où $(m, \ell) \in \mathbb{N}^2$ et où $r > N$ est le $PPCM$ des quatre valeurs possibles du nombre:

$$\Big[\pi - \Big(\frac{D}{\pi}\Big)\Big]\,\Big[\omega - \Big(\frac{D}{\omega}\Big)\Big].$$

On peut noter que r divise donc l'entier $(\pi^2 - 1)\,(\omega^2 - 1)/4$ et lui est même souvent égal, ce qui conduit à donner à r un ordre en $O\,(N^2/4)$.

IV.— Propriétés cryptiques des suites de Lucas

Rassemblons ici les quatre propriétés à mettre en œuvre dans les systèmes cryptographiques utilisant la suite v de Lucas:

$$\begin{array}{|ll|}\hline v_n \circ v_m = v_{nm} & \text{[i]} \\ v_n \circ v_m = v_m \circ v_n & \text{[ii]} \\ v_{mr+1}(p) \equiv p & \text{[iii]} \\ v_{mr+\ell}(p) \equiv v_\ell(p) & \text{[iv]} \\ \hline \end{array}$$

Notons que [ii] (resp. [iii]) découle évidemment de [i] (resp. [iv]).

Rappelons par ailleurs que [iii] signifie de manière précise qu'il existe un indice r tel que l'égalité en question soit vérifiée modulo N pour tout triplet d'entiers (m, p, N) vérifiant les conditions explicitées ci–dessus (une remarque analogue valant naturellement pour [iv]).

Désormais $\mathcal{A}$ *est un anneau de la forme* $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ *où* $N \in \mathbb{N}^*$

V.— Un échange Lucas / Diffie–Hellman

V.1) Etablissement de l'annuaire des clefs publiques.

Si les membres d'un club, parmi lesquels figurent *Alice* et *Bob*, désirent disposer deux à deux de clefs secrètes (pouvant par exemple servir à l'encryptage et au décryptage de messages) sans avoir auparavant à établir de liaisons explicites pour chaque couple, il suffit de publier un annuaire contenant, face à chaque nom de membre, une clef publique construite selon la procédure explicitée ci–dessous.

Le gérant du club choisit et publie, en première page de l'annuaire, un nombre premier impair N, définissant un corps $\mathcal{A} = \mathbb{F}_N$, ainsi qu'un entier p tel que, pour tout diviseur t de $N+1$, $v_{N+1/t}$ soit différent de 2 dans $\mathcal{A}$.

Alice choisit ensuite (et garde secret) un entier $a \in \mathbb{N}^*$, calcule et publie $\alpha = v_a(p)$; *Bob* choisit de son côté (et garde secret) un entier $b \in \mathbb{N}^*$, calcule et publie

$\beta = v_b(p)$ et ainsi de suite. L'annuaire est alors distribué à tous les membres du club.

V.2) Calcul d'une clef secrète commune à Alice et Bob.

Deux membres du club, comme *Alice* et *Bob*, partagent automatiquement une clef qu'aucune autre personne [membres du club compris] ne peut connaître. Il s'agit évidemment de la clef:

$$v_a(\beta) = v_b(\alpha)$$

égale à $v_{ab}(p)$, qu'ils peuvent calculer chacun de leur côté sans qu'il y ait eu à convenir auparavant de quoi que ce soit entre *Alice* et *Bob*.

V.3) Comparaison avec la méthode Diffie–Hellman.

L'égalité fondamentale $v_a(\beta) = v_b(\alpha)$ rappelle, bien entendu, l'égalité $\beta^a = \alpha^b$, où α et β sont respectivement de la forme p^a et p^b [où p engendre le groupe $\mathbb{F}_N^*$] constituant le cœur du système **Diffie–Hellman** d'échange de clefs secrètes à partir de clefs publiques.

Ce n'est naturellement pas un hasard: ici encore, N est premier impair. De plus, la propriété des v_n utilisée pour ce cryptage, à savoir [ii], est également vérifiée par les fonctions $\hat{v}_n$ utilisées dans la méthode initiale de Diffie et Hellman ($\hat{v}_n(x) = x^n$ pour les éléments x d'un groupe commutatif G), puisque la clef commune est de la forme $\hat{v}_a \circ \hat{v}_b(p) = p^{ab} = \hat{v}_b \circ \hat{v}_a(p)$.

VI.— Une signature Lucas / Diffie–Hellman

Il s'agit d'une simple adaptation de la technique d'échange de clef décrite ci–dessus (mais différente du schéma initialement proposé par Diffie et Hellman dans leurs articles originaux). Ici *Alice*, toujours membre du club, désire envoyer un message M (une suite d'au plus N bits, considérée comme élément de $\mathcal{A}$) à *Bob* qui, dans ce cas, est a priori étranger au système, en lui prouvant qu'elle est bien l'auteur du texte.

Ici α, p et N sont donc publics. Dès que *Alice* se manifeste auprès de lui, *Bob* choisit aléatoirement une clef secrète b et lui envoie $\beta = v_b(p)$ [en d'autres termes, tout se passe comme si pour l'occasion *Bob* devenait lui aussi, mais pour un temps seulement, membre du club].

Pour **authentifier** le message M (expédié en clair), *Alice* n'a qu'à l'accompagner d'une **signature** σ, produit dans $\mathbb{F}_N$ de M par $v_a(\beta)$: le contrôle est

immédiat puisque *Bob* n'a qu'à la comparer au produit $M\, v_b(\alpha)$ qu'il obtient sans peine.

Il est trivial d'imaginer mille variantes du scénario : utiliser par exemple des fonctions de compression du message, faire tirer b et en déduire β par *Alice* elle–même, ou remplacer le produit par une somme booléenne bit à bit, etc.

Il est également possible de réunir les deux techniques à la Diffie–Hellman, c'est–à–dire simultanément crypter et signer le message, ou au contraire de se limiter à une simple **identification** d'*Alice* par *Bob*, etc.

VII.— Un cryptage Lucas / RSA

VII.1) Encryptage à l'aide d'une clef publique.

Si *Alice* désire que n'importe qui puisse lui envoyer des messages qu'elle puisse seule déchiffrer, elle commence par publier un entier $N = \pi\,\omega$ comme ci–dessus, indécomposable en un temps raisonnable, et garde secrets les deux nombres π et ω.

Alice calcule ensuite (et garde secret) l'entier r défini plus haut, et publie un entier e premier avec r, tout en déterminant par l'algorithme d'Euclide (et en gardant secret) un entier d tel que $de \equiv 1 \quad [r]$.

Soit *Bob* une personne, dont *Alice* ne connait même peut–être pas l'existence, qui désire lui transmettre une information. Il code son message sous la forme d'un entier p tel que $D = p^2 - 4$ soit premier avec N, l'encrypte sous la forme de l'entier $n = v_e(p) \quad [N]$, et l'expédie à *Alice* (par exemple en recourant à une ligne publique, même peu sûre).

VII.2) Décryptage à l'aide d'une clef secrète.

Dès la réception de n, *Alice* calcule le résidu modulo N de l'entier $v_d(n)\,[= v_d \circ v_e(p) = v_{de}(p)]$. Comme de est de la forme $mr + 1$, il en résulte que $v_d(n)$ est le message p en clair, sans qu'il y ait eu à convenir auparavant de quoi que ce soit entre *Alice* et *Bob*.

VII.3) Comparaison avec la méthode RSA.

L'égalité fondamentale $v_d \circ v_e(p) = v_{de}(p) \equiv p \quad [N]$, sous la condition $de \equiv 1 \quad [r]$, rappelle, bien entendu, l'égalité $(M^e)^d = M^{ed} \equiv M \quad [N]$, sous la condition $de \equiv 1 \quad [\varphi(N)]$ [où φ désigne l'indicateur d'Euler] constituant le cœur du système **RSA** de cryptographie à clef publique.

Ce n'est naturellement pas un hasard : ici encore, N est obtenu comme produit de deux très grands diviseurs premiers impairs distincts. De plus, les propriétés des v_n utilisées pour ce cryptage, à savoir [i] et [iii], sont également vérifiées par les fonctions $\hat{v}_n$ utilisées dans la méthode initiale de **Rivest, Shamir** et **Adleman** ($\hat{v}_n(x) = x^n$ pour les éléments x d'un groupe commutatif G), puisque $\hat{v}_n \circ \hat{v}_m = \hat{v}_{nm}$ et que, dans le cas du groupe des éléments inversibles de l'anneau $\mathbb{Z}_N$, l'entier $r = \varphi(N)$ est tel que $\hat{v}_{mr+1}(x) = x$ pour tout $x \in (\mathbb{Z}_N)^*$.

VIII.— Une signature Lucas / RSA

Ici *Alice* et *Bob* sont membres d'un même club. La première garde secret (π, ω, r, d) et publie (N, e); l'autre agit de même avec (π', ω', r', d') et (N', e'). *Alice* désire expédier à *Bob* un message M à la fois **crypté** et **signé**. Nous prendrons, pour simplifier, $M \in]0, \min(N, N')[$.

Supposons d'abord $N \leq N'$; *Alice* calcule $X \in [0, N[\subset [0, N'[$, reste modulo N de $v_d(M)$, puis expédie $Y' \in [0, N'[$, reste modulo N' de $v_{e'}(X)$.

Pour décrypter et vérifier la signature, *Bob* n'a qu'à calculer $Z' \in [0, N'[$, reste modulo N' de $v_{d'}(Y')$, donc presque sûrement congru modulo N' à X et égal à X, pour retrouver M, reste modulo N de $v_e(Z')$.

Sinon *Alice* calcule $X' \in [0, N'[\subset [0, N[$, reste modulo N' de $v_{e'}(M)$, puis expédie $Y \in [0, N[$, reste modulo N de $v_d(X')$; *Bob* n'a alors qu'à calculer $Z \in [0, N[$, reste modulo N de $v_e(Y)$, donc congru modulo N à X' et égal à X', pour retrouver M, reste modulo N' de $v_{d'}(Z)$.

La preuve de ces affirmations résulte du fait que les produits du type $v_d \circ v_e$ commutent et induisent [avec une probabilité pratiquement égale à 1] l'identité dans des anneaux du type $\mathbb{Z}_N$. On notera que cette signature, reposant sur les propriétés [i] à [iii], est directement issue des idées initiales de Diffie et Hellman préconisant l'utilisation de fonctions d'**encryptage** et de **décryptage** inverses bilatères l'une de l'autre.

IX.— Un cryptage Lucas / ElGamal

IX.1) Encryptage à l'aide d'une clef publique.

Si *Alice* désire que n'importe qui puisse lui envoyer des messages qu'elle puisse seule déchiffrer, elle commence par publier un nombre premier impair N, définissant

un corps $\mathcal{A} = \mathbb{F}_N$, et un entier p tel que, pour tout diviseur t de $N+1$, $v_{N+1/t}(p)$ soit différent de 2 dans $\mathcal{A}$.

Alice choisit ensuite (et garde secret) un entier $a \in \mathbb{N}^*$, calcule et publie $\alpha = v_a(p)$.

Soit *Bob* une personne, dont *Alice* ne connait même peut–être pas l'existence, qui désire lui transmettre une information. Il code son message sous la forme d'un élement $M \in \mathcal{A}$, choisit aléatoirement un entier $k \in \mathbb{N}^*$, puis calcule et expédie à *Alice* (par exemple en recourant à une ligne publique, même peu sûre) le couple:

$$(\lambda, \mu) = (v_k(p), v_k(\alpha)\, M) \in \mathbb{F}_N^2.$$

IX.2) Décryptage à l'aide d'une clef secrète.

Dès la réception de (λ, μ), *Alice* calcule $\gamma = v_a(\lambda) \in \mathbb{F}_N$, égal à $v_a \circ v_k(p) = v_k \circ v_a(p) = v_k(\alpha)$, puis [par l'algorithme d'Euclide] son inverse γ^{-1} et enfin:

$$\gamma^{-1}\, \mu = \gamma^{-1}\, \gamma\, M = M$$

qui est le message en clair, sans qu'il y ait eu à convenir auparavant de quoi que ce soit entre *Alice* et *Bob*.

IX.3) Comparaison avec la méthode ElGamal.

L'égalité fondamentale $M = v_a(\lambda)^{-1}\, \mu$ rappelle, bien entendu, l'égalité $M = \lambda^{-a}\, \mu$, constituant le cœur du système **ElGamal** de cryptographie à clef publique.

Ce n'est naturellement pas un hasard : ici encore, N est premier impair et k est tiré aléatoirement par *Alice*. De plus, la propriété des v_n utilisée pour ce cryptage, à savoir [ii], est également vérifiée par les fonctions $\hat{v}_n$ utilisées dans la méthode initiale d'ElGamal ($\hat{v}_n(x) = x^n$ pour les éléments x du groupe commutatif $\mathbb{F}_N^*$), puisque $\hat{v}_n \circ \hat{v}_m = \hat{v}_n \circ \hat{v}_n$ et que (λ, μ) est également de la forme $(\hat{v}_k(p), \hat{v}_k(a)\, M)$.

Toutefois, la relation $\hat{v}_n \hat{v}_m = \hat{v}_{n+m}$, qui joue un rôle essentiel dans le système de **signature** d'ElGamal et ceux qui en dérivent (comme le **DSA** ou celui de **Schnorr**), n'a pas d'équivalent simple en termes de suite de Lucas, ce qui complique un peu la mise au point d'une signature basée sur v et ElGamal (voir cependant la partie suivante).

X.— Une signature Lucas / ElGamal

X.1) Signature à l'aide d'une clef secrète.

Nous reprendrons naturellement des concepts déjà rencontrés dans les parties précédentes. En particulier N est du type $\pi\omega$ comme au **IX**; ici r sera l'un des quatre nombres $(\pi \pm 1)(\omega \pm 1)$ (et non leur *p.p.c.m.*, donc de l'ordre de N) car la propriété [iv] ne sera utilisée ici que pour un seul $p \in \mathcal{A} = \mathbb{Z}_N$.

Alice, toujours membre du club, désire expédier un message M (une suite d'au plus r bits, considérée comme élément de $\mathbb{N}$) à *Bob* qui, dans ce cas, est *a priori* étranger au système, en lui prouvant le texte est de sa main et transmis sans erreurs.

Ici α et N sont publics, a et r restant le secret d'*Alice*, ainsi éventuellement que p et D dont *Bob* n'aura pas besoin. L'entier a est supposé inférieur à r. Dès que le message est prêt, *Alice* choisit aléatoirement une clef secrète $b \in \mathbb{N}$ inférieure et première à r, calcule l'unique entier $t \in \bar{t} = \beta = v_b(p) \in \mathbb{Z}_N$ inférieur à N ainsi – grâce à l'algorithme d'Euclide étendu – que l'entier $s < r$ tel que sb soit congru à Mta modulo r. Elle expédie alors en clair à *Bob* son message M **signé** par le couple (s, t).

X.2) Authentification à l'aide d'une clef publique.

Dès la réception de (M, s, t), *Bob* calcule l'entier $n = Mt$ et compare $v_n(\alpha)$ à $v_s(\beta) = v_s(\bar{t})$. Comme:

$$v_n(\alpha) = v_{Mt}(\alpha) = v_{Mta}(p) = v_{sb}(p) = v_s(\beta),$$

il peut donc **authentifier** l'intégrité de M et l'identité de son expéditeur sans qu'il y ait eu à convenir auparavant de quoi que ce soit entre *Alice* et *Bob*.

X.3) Une variante intéressante.

Aux calculs d'*Alice*, ajoutons celui de l'entier $z < r$ tel que zs soit congru à 1 modulo r [si s n'est pas inversible dans $\mathbb{Z}_r$, essayer une autre clef b]; la signature est alors (z, t).

Bob calcule maintenant $m = zMt$ et $v_m(\alpha)$ qu'il compare à t puisque:

$$t \in \bar{t} = \beta = v_b(p) = v_{zsb}(p) = v_{zMta}(p) = v_{ma}(p) = v_m(\alpha).$$

Il n'y a donc ici qu'un seul calcul de suite de Lucas à effectuer (au lieu de deux dans la méthode de base); toutefois le bénéfice n'est pas très grand dans la mesure où l'indice m est du même ordre de grandeur que le produit sn des indices utilisés

au **3)**. Cette variante est inspirée de l'une des améliorations apportées par le **DSA** à la technique traditionnelle.

X.4) Comparaison avec la méthode ElGamal.

Pour cette signature inédite évidemment proche du schéma d'ElGamal (mais qui n'en est pas une adaptation triviale), les propriétés des v_n mises en œuvre sont [i] et [iv], cette dernière jouant peu ou prou le rôle de la relation $\hat{v}_n\hat{v}_m = \hat{v}_{n+m}$, moteur essentiel du schéma initial d'ElGamal.

Rappelons qu'on y utilise en effet une signature (s,t) définie par les relations $\alpha = \hat{v}_a(p\,)$, $t \in \beta = \hat{v}_b(p\,)$ et $M \equiv sb + ta \quad [N]$ pour en tirer l'égalité $\hat{v}_M(p\,) = \hat{v}_s(\beta)\,\hat{v}_t(\alpha)$.

Il est trivial d'imaginer mille variantes du scénario, et également possible de réunir les deux techniques, c'est–à–dire simultanément crypter et signer le message, ou au contraire de se limiter à une simple **identification** d'*Alice* par *Bob*, etc.

XI.— Une signature Lucas / DSA

L'algorithme de signature du **DSA** l'emporte notamment sur celui d'ElGamal par le raccourcissement de la signature. On peut agir dans ce sens avec une suite de Lucas en procédant par exemple de la manière suivante : un premier choix de p conduisant à un entier r de la forme $(\pi \pm 1)\,(\omega \pm 1)$, on peut remplacer (p,r) par (p',r') avec $r' = \pi'\omega' < r$, où π' est un diviseur premier de $\pi \pm 1$, ω' un diviseur premier de $\omega \pm 1$ et $p' = v_{r/r'}(p\,)$, puisqu'alors $v_{r'}(p') = v_r(p\,) = \bar{2}$.

Le plus petit entier m tel que $v_m(p') = \bar{2}$ est un diviseur de r'; si $m \neq r'$, c'est qu'il vaut 1, π' ou ω'. Il est donc très facile, en changeant au besoin de p, d'obtenir $m = r'$. La signature (s,t) [éventuellement (z,t)] est alors formée d'un entier sur r' bits au plus et d'un autre sur N bits, ce qui consitue un gain appréciable de l'ordre de $r - r'$ bits.

Bien entendu, dans la pratique, la démarche est inversée : on se donne d'abord π' et ω', puis $\pi = 2\,\lambda\pi' \pm 1$, $\omega = 2\,\mu\omega' \pm 1$ et $N = \pi\omega$ avant de trouver p et p' associé à des signatures plus courtes que par la méthode de base, mais suffisamment longues pour conserver un haut niveau de sécurité.

XII.— Suites multiplicatives de Rédei

XII.1) Suites multiplicatives.

Nous appellerons ici *suite multiplicative* toute suite s de fonctions vérifiant, comme v, l'identité:

$$\boxed{s_{nm} = s_n \circ s_m}$$

Leur application en cryptographie est claire d'après les parties précédentes. Nous connaissons deux autres cas, très simples, de telles suites : $\hat{v}$, définie par $\hat{v}_n(p\,) = p^n$, et bien évidemment μ, définie par $\mu_n(p\,) = n\,p$.

Voici une construction systématique de suites multiplicatives: à partir d'une solution s, on en obtient évidemment une autre σ par *conjugaison*, c'est–à–dire en *transmuant* s par une bijection φ:

$$\sigma = \varphi \circ s \circ \varphi^{-1}.$$

Si $s = \mu$, on obtient le cas particulier $\sigma_n(p\,) = \varphi\left(n\,\varphi^{-1}(p\,)\right)$.

En un certain sens, la suite v de Lucas relève de cette technique si l'on veut bien se rappeler la relation de TCHEBITCHEFF dans $\mathbb{C}$:

$$v_n(p\,) = 2\,\cos\left[n\,\text{Arc}\,\cos\frac{p}{2}\right] = 2\,\cos n\theta$$

pour $p = \varphi\,(\theta) = 2\,\cos\theta$.

XII.2) La suite de RÉDEI.

Acceptant de fermer encore un instant les yeux sur le fait que les fonctions trigonométriques ne sont qu'imparfaitement bijectives, il peut para ître naturel de continuer dans cette voie afin d'obtenir de nouvelles suites multiplicatives algébriques chaque fois que $\varphi\,(nt)$ s'exprime rationnellement en fonction de $\varphi\,(t)$. C'est sans doute ce qu'a fait L. Rédei en 1946 en introduisant des fractions rationnelles R_n, dépendant d'un paramètre α, satisfaisant à l'égalité fondamentale:

$$R_n(p\,) = \sqrt{\alpha}\,\coth\left[n\,\text{Arg}\,\coth\frac{p}{\sqrt{\alpha}}\right] = \sqrt{\alpha}\,\coth n\theta$$

pour $p = \sqrt{\alpha}\,\coth\theta$.

A partir de l'égalité $e^{2\theta} = \dfrac{\coth\theta + 1}{\coth\theta - 1}$, on peut donner une expression explicite:

$$R_n(p\,) = \sqrt{\alpha}\,\frac{(p+\sqrt{\alpha}\,)^n + (p-\sqrt{\alpha}\,)^n}{(p+\sqrt{\alpha}\,)^n - (p-\sqrt{\alpha}\,)^n} = \frac{\sum C_n^{2k}\,\alpha^k\,p^{n-2k}}{\sum C_n^{2k+1}\,\alpha^k\,p^{n-2k-1}}$$

(les sommations portent sur les entiers naturels respectivement tels que $2k \leq n$ et $2k < n$).

On peut mettre cette relation sous une forme telle que l'identité fondamentale $R_n \circ R_m = R_{nm}$ est alors presque en évidence:

$$\frac{R_n(p\,) + \sqrt{\alpha}}{R_n(p\,) - \sqrt{\alpha}} = \left(\frac{p + \sqrt{\alpha}}{p - \sqrt{\alpha}}\right)^n.$$

XII.3) Définition des suites g, h et R **de Rédei**.

a) Dans tout anneau commutatif (unitaire) $\mathcal{A}$ on peut définir à partir d'un élément $\alpha \in \mathcal{A}$ deux suites de polynômes $(g_n,\, h_n)$ par les égalités:

$$g_n(X) = \sum_{k=0}^{[n/2]} C_n^{2k}\, \alpha^k\, X^{n-2k}, \qquad h_n(X) = \sum_{k=0}^{[(n-1)/2]} C_n^{2k+1}\, \alpha^k\, X^{n-2k-1}.$$

b) On peut encore les obtenir par une égalité matricielle directe:

$$\begin{pmatrix} g_n(X) & \alpha\, h_n(X) \\ h_n(X) & g_n(X) \end{pmatrix} = \begin{pmatrix} X & \alpha \\ 1 & X \end{pmatrix}^n$$

ou, de manière récurrente, par les données $(g_0(X) = 1,\, h_0(X) = 0)$ et les relations:

$$g_{n+1}(X) = X\, g_n(X) + \alpha\, h_n(X), \qquad h_{n+1}(X) = g_n(X) + X\, h_n(X),$$

voire par les données $(g_0(X) = 1,\, g_1(X) = X,\, h_0(X) = 0,\, h_1(X) = 1)$ et les relations d'ordre 2:

$$g_{n+2}(X) = 2\, X\, g_{n+1}(X) + (\alpha - X^2)\, g_n(X),$$
$$h_{n+2}(X) = 2\, X\, h_{n+1}(X) + (\alpha - X^2)\, h_n(X).$$

Cela montre que g_n et h_n sont des cas particuliers de suites originelles de Lucas définies par la relation $L_{n+2} = p\, L_{n+1} - q\, L_n$ $(p = 2\, X,\, q = X^2 - \alpha)$.

c) Il est également facile de déduire de la définition matricielle les formules suivantes d'*addition* et de *duplication*:

$$g_{n+m}(X) = g_n(X)\, g_m(X) + \alpha\, h_n(X)\, h_m(X),$$
$$h_{n+m}(X) = h_n(X)\, g_m(X) + \quad g_n(X)\, h_m(X),$$
$$g_{2n}(X) = g_n^2(X) + \alpha\, h_n^2(X), \qquad h_{2n}(X) = 2\, g_n(X)\, h_n(X).$$

Notons également les égalités:

$$X\, g_{n+1} - \alpha\, h_{n+1} = (X^2 - \alpha)\, g_n, \quad X\, h_{n+1} - g_{n+1} = (X^2 - \alpha)\, h_n.$$

Un calcul immédiat de déterminant montre par ailleurs que:

$$g_n^2(X) - \alpha\, h_n^2(X) = (X^2 - \alpha)^n.$$

d) S'il existe $\beta \in \mathcal{A}$ tel que $\beta^2 = \alpha$, g_n et h_n vérifient évidemment les égalités $g_n(\beta) = 2^{n-1}\,\beta^n,\ h_n(\beta) = (2\,\beta)^{n-1}$ ainsi que:

$$g_n(X) + \beta\, h_n(X) = (X+\beta)^n, \qquad g_n(X) - \beta\, h_n(X) = (X-\beta)^n$$

qui redonnent aussitôt la relation précédente.

e) Pour définir la fraction rationnelle $\boxed{R_n = \dfrac{g_n}{h_n}}$ nous supposerons désormais que l'anneau $\mathcal{A}$ est un **corps commutatif** noté K.

Le cas particulier $\alpha = 0$ est sans grand interêt, puisque l'on a alors immédiatement $g_n(X) = X^n$ et $h_n(X) = n\,X^{n-1}$; nous l'écarterons par conséquent. Soit donc $\alpha \neq 0$. S'il existe un entier n tel que $h_n(X) = 0$, c'est que tous les coefficients C_n^{2k+1} sont nuls dans K; les développements de $(1-1)^n$ et $(1+1)^n$ donnant alors $0 = 2^n$, K est de caractéristique 2 et $h_{2m} = 0,\ h_{2m+1} = g_{2m} = (X^2+\alpha)^m,\ g_{2m+1} = X\,(X^2+\alpha)^m$. Nous écarterons également ce cas pour qu'aucun h_n ne soit nul.

XII.4) Propriétés de la suite R de Rédei.

a) Soit donc maintenant $\mathcal{A} = K$, corps comuutatif de caractéristique différente de 2, et $\alpha \in K^*$; la fraction $R_n = \dfrac{g_n}{h_n} \in K(X)$ est alors définie pour tout $n \in \mathbb{N}^*$ et vérifie notamment les égalités simples:

$$R_{n+m} = \frac{R_n\,R_m + \alpha}{R_n + R_m}, \quad R_{n+1} = \frac{X\,R_n + \alpha}{R_n + X}, \quad R_{2n} = R_2 \circ R_n = \frac{R_n^2 + \alpha}{2\,R_n}$$

conduisant classiquement à un algorithme de calcul de R_n basé sur une technique analogue à une "exponentiation rapide" facile à expliciter.

b) Montrons à l'aide de l'égalité $g_n^2 - \alpha\, h_n^2 = (X^2-\alpha)^n$ que les polynômes g_n et h_n sont maintenant *premiers entre eux*. En effet tout diviseur non trivial de g_n et h_n devrait posséder, dans une extension convenable de K, une racine β vérifiant $\beta^2 = \alpha \neq 0$ et les égalités impossibles $0 = g_n(\beta) = 2^{n-1}\,\beta^n,\ 0 = h_n(\beta) = (2\,\beta)^{n-1}$.

c) Pour $K = \mathbb{C}$ et $\alpha > 0$, les racines de h_n sont les $n-1$ complexes:

$$i\,\sqrt{\alpha}\,\operatorname{cotg}\frac{k\pi}{n} \qquad (0 < k < n)$$

parmi lesquelles ne figure un réel (0) que si et seulement si n est pair. Celles de g_n sont les n complexes:

$$i\sqrt{\alpha}\ \mathrm{cotg}\ \frac{(2\,k+1)\,\pi}{2\,n} \qquad (0 \le k < n)$$

parmi lesquelles ne figure un réel (0) que si et seulement si n est impair.

Pour $\alpha < 0$, on obtiendrait respectivement:

$$\sqrt{-\alpha}\ \mathrm{cotg}\ \frac{k\pi}{n} \qquad (0 < k < n)$$

$$\sqrt{-\alpha}\ \mathrm{cotg}\ \frac{(2\,k+1)\,\pi}{2\,n} \qquad (0 \le k < n)$$

donnant $n-1$ pôles et n zéros, tous simples et réels, à R_n.

d) Le calcul de la dérivée $R_n^{'}$ repose sur le wronskien:

$$h_n(X)\,g_n'(X) - g_n(X)\,h_n'(X) = n\,(X^2-\alpha)^{n-1}$$

qui s'obtient par une banale récurrence. La relation:

$$R_n^{'}(X) = n\,\frac{(X^2-\alpha)^{\,n-1}}{h_n^2(X)}$$

s'en déduit aussitôt, ainsi que les variations de R_n pour $\alpha \in K = \mathbb{R}$: s'il existe d'éventuels extremums de R_n, ils sont égaux à $\pm\sqrt{\alpha}$ (qui existe) et n est pair; sinon R_n croît strictement sur chaque composante connexe de son ensemble de définition ($\mathbb{R}$ si $\alpha > 0$ et n impair).

XIII.— Commentaires bibliographiques

On pourra trouver une introduction très simple aux problèmes de cryptographie moderne (et, en particulier, à clef publique) dans l'excellent:

CRYPTOLOGIE CONTEMPORAINE par G. Brassard, Masson 1992, coll. LMI (ainsi que sa version anglaise, moins complète, parue en 1988 chez Springer Verlag sous le titre *Modern Cryptology*). La somme de références bibliographiques que l'on y trouve (livres et articles) est impressionnante, ainsi que le savoir–faire de l'auteur, qui réussit à faire comprendre avec toute la précision nécessaire la structure essentielle des processus engagés sans recourir à une seule équation.

À un niveau technique plus élaboré, bien que restant modeste, les meilleures références figurent sans aucun doute dans les deux compilations:

CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY sous la direction de G.J. SIMMONS, IEEE Press, Piscataway 1992.

APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C par BRUCE SCHNEIER, John Wiley and Sons 1993.

D'après ce dernier auteur, l'idée de recourir aux suites de Lucas (éventuellement élargies en polynômes de Dickson et suites de Rédei) est due à de nombreux chercheurs, dont LIDL, MÜLLER et NÖBAUER, ainsi qu'au Néo–Zélandais PETER SMITH qui, en 1993, redécouvrit le schéma de base et créa divers logiciels comme LUC, LUCDIF, LUCELG PK et LUCELG DS.

Sur les propriétés mathématiques des suites de Lucas elles–mêmes, l'ouvrage essentiel, contenant plusieurs paragraphes consacrés à leur utilisation en cryptographie (ainsi d'ailleurs que celle des suites de Rédei), est le récent:

DICKSON POLYNOMIALS par R. LIDL, G.L. MULLEN et G. TURNWALD, Longman Scientific and Technical 1993, Pitman Monographs in Pure and Applied Mathematics (dirigées par H. Brezis, R. G. Douglas et A. Jeffrey).

L'origine de leur étude est à rechercher dans la référence donnée plus haut (CRAS), ainsi que dans les deux articles séminaux cités ci–dessous:

Références

1. D.H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math.* **31** (1930), 419–448.
2. E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240 et 289–321.