PÉRIODICITÉ DE LA SUITE DE FIBONACCI

FRANÇOIS CROS, JONATHAN DUPEUX ET JOHANN MILON

Remerciements à Mr A.Necer, pour l'encadrement de ce projet d'initiation à la recherche

Résumé. Ce document traite de la période de la suite de Fibonacci à l'aide de l'étude de ses valeurs propres. Il contient les définitions, théorèmes et exemples essentiels quant à la compréhension de ce sujet.

Table des matières

Date: Février 09, 2017.
Key words and phrases. Fibonacci, Récurrence, Résidus Quadratiques, Période.

1. Introduction

Nous allons commencer par définir ce qu'est la suite de Fibonacci.
La suite de Fibonacci est une suite d'entiers dans laquelle chaque terme est la somme des termes qui le précédent. Elle peut s'écrire sous cette forme :
$\forall\ n \geq 0, \mathbf{U}_{n+2} = \mathbf{U}_{n+1} + \mathbf{U}_n$ Avec $U_0 = 0$ et $U_1 = 1$.

Cependant, nous allons réduire les termes de cette suite modulo un entier m premier c'est-à-dire étudier la suite sur $\mathbb{Z}/m\mathbb{Z}$.
Nous pouvons remarquer qu'il y aura dans ce cas m^2 paires d'éléments consécutifs possibles. Ce qui signifie que si l'on calcule un nombre élevé de termes alors on va finir par retomber sur une paire d'éléments déjà trouvée auparavant et comme une paire d'éléments dépend de la paire qui l'a précéde alors on va finir par réobtenir les mêmes termes de la suite.
On peut donc en déduire que notre suite sera **périodique**.
La borne supérieure de cette période est $m^2 - 1$ (car il y a m^2 paires possibles mais il faut retirer la paire (0,0) qui n'existe pas, on ne peut avoir 2 zéros à la suite).
Or, nous remarquons que la majorité du temps la période est bien inférieure à $m^2 - 1$.
Exemple : m = 19. On calcule les différents termes de la suite :

0,1,1,2,3,5,8,13,2,15,17,13,11,5,16,2,18,1,0,1,1 ...

On a une période ici qui est égal à 18.

Les mathématiciens Wall et Robinson, qui ont étudié les périodes de cette suite dans les années 60, ont montré que si on prenait un nombre premier $p \equiv 2, 3[5]$ la période de la suite divise 2(p+1) et si $p \equiv 1, 4[p]$ la période divise $p - 1$.

Le but de notre projet va être de démontrer les travaux de Wall et Robinson sur la périodicité des suites de Fibonacci.

Notre exposé va être divisé en deux parties, une première partie théorique de démontrations et une partie expérimentale calculatoire afin de donner des exemples pour illustrer notre première partie.

2. Définitions importantes

Avant toutes choses nous allons énnoncer quelques définitions et propriétés essentielles à la résolutions des théorèmes à venir.

2.1. **Résidus quadratiques.**

Définition 1. *Soit p un nompre premier et a un entier tel que p ne divise pas a. Alors a est appelé résidu quadratique mod p si l'équation :*

$$x^2 \equiv a[p]$$

possède une solution.
Autrement dit, a est un résidu quadratique si et seulement si a mod p est un carré dans $(\mathbb{Z}/p\mathbb{Z})$.

Proposition 1. *On dit que a est un résidu quadratique si et seulement si :*

$$a^{\frac{p-1}{2}} \equiv 1[p]$$

Si non on dira que a est un nonrésidu quadratique et :

$$a^{\frac{p-1}{2}} \equiv -1[p]$$

2.2. **Période d'une suite.**

Définition 2. *On appelle période modulo p d'une suite U l'élément T tel que :*

$$\forall n \in \mathbb{N},\ U_{n+T}\ mod(p) \equiv U_n\ mod(p)$$

La période $k_{A,B}(p)$ divise tout n qui vérifie $\mathrm{D}^n = I$

3. Les valeurs propres de la matrice de Fibonacci

Rappel 1. *Rappelons pour commencer qu'une suite récurrente linéaire d'ordre k sur un corps commutatif K est une suite définie par une relation de récurrence du type :*
$u_{n+k} = a_{k-1}.u_{n+k-1} + ... + a_0.u_n$
avec $a_0, ..., a_{n+k-1}$ *dans K,et pour* $u_0, ..., u_{k-1}$ *fixés*

On remarque alors que la suite de Fibonacci est une suite récurrente linéaire d'ordre 2 avec :

$$a_0 = 1, a_1 = 1, u_0 = 1, u_1 = 2$$

Soit p un nombre premier tel que $p \geq 2$.

Notation 1. *On note k(p) la période de la suite de Fibonacci modulo p, qui est le plus petit i tel que* $F_i \equiv 0 \pmod{p}$ *et* $F_{i+1} \equiv 1 \pmod{p}$.

Rappel 2. *Le polynôme caractéristique associé à une suite récurrente linéaire*
$u_{n+k} = a_{k-1}.u_{n+k-1} + ... + a_0.u_n$ *est le polynôme :*
$P(X) = X^k$ - $a_{k-1}.X^k - 1$ - ... - $a_1.X - a_0$

Le polynôme caractéristique associé à la suite de Fibonacci $U_{n+2} = U_{n+1} + U_n$ sera donc :

$$X^2 \text{ - } X \text{ - } 1.$$

Rappel 3. *La matrice compagnon d'un polynôme unitaire*
$P(X) = X^n + k_{n-1}.X^{n-1} + ... + k_0$
est la matrice carrée suivante :

$$A = \begin{pmatrix} -k_{n-1} & -k_{n-2} & ... & -k_1 & -k_0 \\ 1 & 0 & ... & 0 & 0 \\ 0 & 1 & ... & 0 & 0 \\ ... & .... & .... & ... & 0 \\ 0 & 0 & ... & 1 & 0 \end{pmatrix}$$

Notation 2. *On note U la matrice compagnon du polynôme caractéristique cité auparavant, appelée aussi matrice de Fibonacci :*

$$U = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

De manière générale, nous pouvons écrire :

$$\mathrm{U}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}$$

Les valeurs propres de U sont les racines du polynôme caractéristique : X^2 - X - 1.
On les notes λ_1 et λ_2.
Si ces deux valeurs propres existent dans $\mathbb{F}_p$, alors nous pouvons diagonaliser notre matrice U, elle sera alors de la forme : $\mathrm{U} = \mathrm{CDC}^{-1}$, où D est la matrice diagonale :

$$\mathrm{D} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

C étant la matrice qui contient les vecteurs propre sur ses colonnes.

Lemme 1. *La période k(p) divise n'importe quel n tel que* $D^n = I$

Démonstration. Nous avons D :

$$\begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$$

Si λ_1 et λ_2 existent dans $\mathbb{F}_p$ alors Δ est un carré.
Si Δ est un carré alors cela signifie que p $\equiv$ 1, 4 (mod 5) (voir démonstration juste au-dessus).
Alors, k(p) | (p-1) qui va être l'ordre. Or, nous savons que $\lambda_{1,2}^{p-1} = 1$. Et donc, si $D^n = \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix}$ $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ Alors n = k(p-1) avec k $\in \mathbb{Z}$. Comme k(p) divise p-1 alors k(p) va diviser n.

□

Théorème 1. *Soit p est un nombre premier impair, si p $\equiv$ 1,4 (mod) p, alors k(p) divise p-1. En particulier, k(p) $\leq$ p-1.*

Démonstration. Nous avons comme polynôme caractéristique : $X^2 - X - 1$

Notre discriminant sera donc : $\Delta = (-1)^2 - 4.1.(-1) = 5$.

La question est de savoir si 5 est un carré dans F_p

Nous allons donc nous retrouver dans deux cas :
1) $p \equiv 0, 1, 4 \pmod 5$
2)p$\equiv 2, 3 \pmod 5$
Ici nous nous focaliserons uniquement sur le cas numéro 1, il y aura 3 sous-cas :

$$\begin{aligned}
&* \text{ Si p } \equiv 0[5] \Rightarrow \left(\tfrac{p}{5}\right) \\
&\qquad = \left(\tfrac{0}{5}\right) \\
&\qquad = 0 \\
&* \text{ Si p } \equiv 1[5] \Rightarrow \left(\tfrac{p}{5}\right) \\
&\qquad = \left(\tfrac{1}{5}\right) \\
&\qquad = 1 \\
&* \text{ Si p } \equiv 4[5] \Rightarrow \left(\tfrac{p}{5}\right) \\
&\qquad = \left(\tfrac{4}{5}\right) \\
&\qquad = \left(\tfrac{2}{5}\right).\left(\tfrac{2}{5}\right) \\
&\qquad = (-1)^{\frac{5^2-1}{8}}.(-1)^{\frac{5^2-1}{8}} \\
&\qquad = (-1)^{\frac{24}{8}}.(-1)^{\frac{24}{8}} \\
&\qquad = (-1).(-1) \\
&\qquad = 1
\end{aligned}$$

Nous pouvons voir que dans ce cas que 5 est un carré dans F_p.

Dans ce premier cas, nous avons démontré l'existence des valeurs propres : λ_1 et λ_2.
D'aprés le petit théorème de Fermat, nous avons : $\lambda^{p-1} \equiv 1 \pmod{}$ p. Nous savons que la période de la suite que l'on note k(p) (ce qui correspond à l'ordre de lambda) divise l'ordre de p. Et donc k(p) divise p - 1.
Nous devons à présent aborder un cas qui "se passe un peu moins bien" étant donné que nous allons devoir utiliser l'extension $\mathbb{F}_p$ de degré 2 afin d'obtenir un résultat intéressant. □

4. Cas particulier : p = 5

Si on a p = 5, alors le polynôme X^2 - X - 1 possédera une racine **double** qui sera 3.

$$3^2 \text{ - } 3 \text{ - } 1 = 9 \text{ - } 3 \text{ - } 1 = 5 = 0$$

On pose : $U = CDC^{-1}$, or $D^p - 1 = D^4 \neq I_4$. Même si ${\lambda_1}^4 = {\lambda_2}^4 = 3^4 = 81 = 1$. Ici,

$$U^4 = \begin{pmatrix} 2 & 3 \\ 3 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La période n'est donc pas 4. On va donc calculer les premiers termes de la suite (grâce au programme Maple présenté en dernière partie).
On trouve une période k(p) = 20.
En effet,

$$U^{20} = \begin{pmatrix} 4181 & 6765 \\ 6765 & 10946 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

La période de la suite de Fibonacci pour p = 5 est 20.

5. Extension du corps pour les valeurs propres

En effet, si on a p $\equiv$ 2,3 (mod) 5, alors dans ce cas, le polynôme X^2 - X - 1 sera irréductible sur $\mathbb{F}_p$. On note alors γ une racine de ce polynôme et avec elle, on construit $\mathbb{F}_{p^2} = \{$ a + bγ tel que a,b $\in \mathbb{F}_p$ $\}$ qui est une extension de $\mathbb{F}_p$ de degré 2. Il s'agit de l'unique corps fini à p^2 éléments.
On a : γ^2 - γ - 1 = 0.
Par la suite, on peut en déduire :

$$\begin{aligned}&(1\text{-}\gamma)^2 - (1-\gamma) \text{ - } 1\\ &= 1 \text{ - } 2.\gamma + \gamma^2 + \gamma \text{ - } 2\\ &= \text{-}1 \text{ - } \gamma + 1 + \gamma = 0\end{aligned}$$

Donc $\bar{\gamma} = 1 - \gamma$ est une autre racine de X^2 - X - 1.
On note aussi que : $\bar{\gamma}.\gamma = \gamma.(1\text{-}\gamma) = \gamma - \gamma^2 = -1$.

Proposition 2. $\forall(x,y) \in F_{p^2}$, $(x + y)^p = x^p + y^p$

Démonstration. En effet, $(x + y)^p = \sum_{k=0}^{p} \binom{p}{k}.x^k.y^{p-k}$

Sachant que :

$$\begin{aligned}\binom{p}{k} &= \frac{p!}{k!(p-k)!}\\ &= \frac{p}{k}\cdot\frac{(p-1)!}{(p-k)!(k-1)!}\\ &= \frac{p}{k}\cdot\binom{p-1}{k-1}\end{aligned}$$

D'où, $k.\binom{p}{k} = p.\binom{p-1}{k-1}$
Donc, $p \mid k.\binom{p}{k}$
Or, p est premier, d'où PGCD(p,k) = 1.
On en déduit que $p \mid \binom{p}{k}$
On en conclut finalement que : $(x + y)^p = x^p + y^p$ □

Lemme 2. *Si P(x) est un polyôme irréductible sur $\mathbb{F}_p$ et γ une racine dans $\mathbb{F}_{p^2}$, alors γ^p est une racine différente dans P(x).*

Démonstration. Soit P(x) = $\sum_{k=0}^{n} a_k.x^k$ avec $a_k \in \mathbb{F}_p$ et γ racine de P.
Alors :

$$\begin{aligned}P(\gamma^p) &= \sum_{k=0}^{n} a_k.\gamma^{p.k}\\ &= \sum_{k=0}^{n} a_k^p.\gamma^{p.k} \text{ (petit théorème de Fermat)}\\ &= (\sum_{k=0}^{n} a_k.x^k)^p \text{ (voir proposition ci-dessus)}\\ &= P(\gamma)^p\\ &= 0\end{aligned}$$

Donc γ^p est racine de P. De plus, $\gamma^p \neq \gamma$ car l'équation x^p = x a au plus p solutions qui sont des élèments de $\mathbb{F}_p$. Or $\gamma \notin \mathbb{F}_p$. Donc $x^p = x$ n'a pas de solutions ce qui entraîne bien que $\gamma^p \neq \gamma$. □

Théorème 2. *Soit p un nombre premier $\geq$ 2, tel que p $\equiv$ 2,3 (*mod *) 5. Alors k(p) divise 2(p+1). Et en particluier, on a k(p) $\leq$ 2(p+1).*

Démonstration. En appliquant le lemme 4 et par le fait que $\gamma.\bar{\gamma}$ = -1, on a :
$\gamma^{2(p+1)} = (\gamma^p)^2.\gamma^2 = (\bar{\gamma})^2.\gamma^2 = (\text{-}1)^2 = 1$.

De même, on a : $(\bar{\gamma})^{2(p+1)} = 1$. On en conclut alors que $D^{2(p+1)} = I$. D'après le lemme 1, k(p) | n tel que $D^n = I$, donc k(p) | 2(p+1). □

6. Récurrence générale

Résumé. Dans cette section nous énoncerons des théorèmes et propriétés utiles aux calculs de la périodicité d'une suite récurrente générale.

6.1. **Introduction à la récurrence générale.** Nous allons approfondir l'étude de la période de la réccurence générale d'une suite de Fibonacci définie comme suit :

$$E_{n+1}{=}AE_n{+}BE_{n-1}$$

modulo un nombre premier p, en posant $E_0{=}0$ et $E_1{=}1$. On appellera $k_{A,B}(\mathrm{p})$ la période de E_n mod p. La nouvelle matrice de Fibonacci devient :

$$\mathrm{U}{=}\begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix}$$

6.2. **Matrice de Fibonacci d'ordre quelconque.**

Proposition 3. *Soit* $\boldsymbol{U}$ *la matrice de Fibonacci définie dans l'introduction, si l'on se place sur* $F{=}\mathbb{R}$ *on a :*

$$U^n = \begin{bmatrix} E_{n+1} & E_nB \\ E_n & E_{n-1}B \end{bmatrix}$$

Démonstration. (par récurrence) Pour n=1

$$\begin{bmatrix} \mathrm{E}_2 & \mathrm{E}_1B \\ \mathrm{E}_1 & \mathrm{E}_0B \end{bmatrix} = \begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix}$$

Comme $\mathrm{E}_2 = A\mathrm{E}_1{+}\mathrm{B}E_0{=}\mathrm{A}$, la propriété est donc vérifiée pour n=1. On suppose maintenant que la propriété est vrai au rang n, c'est à dire que :

$$\mathrm{U}^n = \begin{bmatrix} \mathrm{E}_{n+1} & \mathrm{E}_nB \\ \mathrm{E}_n & \mathrm{E}_{n-1}B \end{bmatrix}$$

Montrons maintenant qu'elle est aussi vrai au rang *n+1.*

$$\begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix}^{n+1} = \begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix}^{n} \times \begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix}$$

Ce qui nous donne :

$$\begin{bmatrix} \mathrm{E}_{n+1} & \mathrm{E}_nB \\ \mathrm{E}_n & \mathrm{E}_{n-1}B \end{bmatrix} \times \begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \mathrm{E}_{n+1}\mathrm{A}{+}E_n\mathrm{B} & \mathrm{E}_{n+1}B \\ \mathrm{E}_n\mathrm{A}{+}E_{n-1}\mathrm{B} & \mathrm{E}_nB \end{bmatrix}$$

En utilisant la définition de la suite récurrente E_n dans l'introduction on peut remplacer les membres à gauche de cette matrice par :

$$\begin{bmatrix} \mathrm{E}_{n+2} & \mathrm{E}_{n+1}B \\ \mathrm{E}_{n+1} & \mathrm{E}_nB \end{bmatrix}$$

. Car E_{n+2}=E_{n+1}A+E_nB. Ceci cloture la preuve de cette proposition. □

6.3. **Théorèmes fondamentaux.**

Théorème 1. *Si p est un nombre premier impair et* Δ *un résidu quadratique non nul mod p, alors* $k_{A,B}(p)$ *divise p-1. De plus* $k_{A,B}(p) \leq p-1$

Démonstration. Le polynome caractéristique de la matrice **U** est

$$X^2 - AX - B$$

, Δ=A^2+4B comme Δ est un résidu quadratique non nul mod p, il existe un δ tel que δ^2 =Δ autrement dit, δ=$(A^2+4B)^{\frac{1}{2}}$. Si on élève ceci à la puissance p-1 on obtient :

$$\delta^{p-1}=(A^2+4B)^{\frac{p-1}{2}} \equiv 1[p] \text{ (par la proposition 1 du (2.1)).}$$

Les valeures propres de la matrice **U** sont repectivement λ et $\overline{\lambda}$ avec :

$$\lambda=\frac{A-\delta}{2} \text{ et } \overline{\lambda}=\frac{A+\delta}{2}$$

En les élevant à la puissance p et en étant en caractéristique p on obtient :

$$\lambda^p=\frac{A^p-\delta^p}{2^p}$$

Or comme δ est d'ordre p-1 δ^p=δ. En utilisant le théorème de Fermat :

$$\begin{array}{ccccccc} 2^{p-1} & \equiv & 1[p] & => & 2^p & \equiv & 2[p] \\ A^{p-1} & \equiv & 1[p] & => & A^p & \equiv & A[p] \end{array}$$

ceci implique que λ^p=$\frac{A-\delta}{2}$=λ, d'ou λ^{p-1}=1.

En mettant **U** sous la forme CDC^{-1} on à :

$$\text{U}=C \times \begin{bmatrix} \lambda & 0 \\ 0 & \overline{\lambda} \end{bmatrix} \times C^{-1}$$

donc

$$U^{p-1}=C \times \begin{bmatrix} \lambda^{p-1} & 0 \\ 0 & \frac{}{\lambda^{p-1}} \end{bmatrix} \times C^{-1}=C \times \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \times C^{-1} = I$$

La matrice **U** est donc d'ordre p-1.

Comme $U^n = \begin{bmatrix} \text{E}_{n+1} & \text{E}_n B \\ \text{E}_n & \text{E}_{n-1} B \end{bmatrix}$
par la proposition 2, il s'en suit que :

$$U^{p-1} = \begin{bmatrix} \text{E}_p & \text{E}_{p-1} B \\ \text{E}_{p-1} & \text{E}_{p-2} B \end{bmatrix} = I,$$

Donc E_p=1 ce qui implique que E_n est au plus de période p-1 (0 étant le premier terme de la suite). Pour conclure, comme $U^{p-1} = I$ par le lemme 1 la période $k_{A,B}$ divise tout n qui vérifie $D^n = I$ donc la période divise p-1. □

Si Δ est un nonrésidu quadratique mod p alors $(\sqrt{\Delta})^p$ = -$(\sqrt{\Delta})$.

Démonstration. En utilisant la proposition 1, comme Δ est un nonrésidu quadratique on à $\Delta^{\frac{p-1}{2}} \equiv -1[p]$. Posons $\delta^2 = \Delta$, cela nous donne que $\delta = (A^2+4B)^{\frac{1}{2}}$, en élevant à la puissance p-1 on a :

$$\delta^{p-1} = \Delta^{\frac{p-1}{2}} = \text{-1 d'ou } \delta^p = -\delta.$$

□

Proposition 4. *Si Δ est un nonrésidu quadratique mod p alors $\lambda^p = \overline{\lambda}$ avec $(\lambda, \overline{\lambda})$ les racines du polynôme caractéristique de U*

Démonstration. On a $\lambda = \frac{A-\delta}{2}$, en élevant à la puissance p on a : $\lambda^p = \frac{A^p - \delta^p}{2^p}$ en utilisant le théorème de Fermat sur A et 2 et en utilisant le lemme précédent sur δ ($\delta^p = -\delta$) on obtient que :

$\lambda^p = \frac{A^p - \delta^p}{2^p} = \frac{A+\delta}{2} = \overline{\lambda}$. □

Théorème 2. *Si Δ est un nonrésidu quadratique mod p, alors :*

$$k_{A,B}(p) \text{ divise } 2(p+1) \times ord(B^2).$$

Démonstration. Tout dabord, il faut voir que $\lambda \times \overline{\lambda} = B^2$.(facilement vérifiable en utilisant $\lambda = \frac{A+\delta}{2}$). Maintenant élevons à la puissance 2(p+1).

$$\begin{array}{rcl} \lambda^{2(p+1)} & = & (\mathrm{A}+\delta_{\overline{2}})^{p+1} \times (\frac{A+\delta}{2})^{p+1} \\ \lambda^{2(p+1)} & = & (\mathrm{A}+\delta_{\overline{2}})^{p} \times (\frac{A+\delta}{2})^{p} \times (\frac{A+\delta}{2})^{2} \end{array}$$

En utilisant le résultat de la proposition 3 ($\lambda^p = \overline{\lambda}$) on a :

$$\lambda^{2(p+1)} = (\overline{\lambda}^2 \times \lambda^2) = B^2.$$

La matrice $U^{2(p+1)}$ devient donc :

$$U^{2(p+1)} = C \times \begin{bmatrix} B^2 & 0 \\ 0 & B^2 \end{bmatrix} \times C^{-1}.$$

On remarque tout de suite que si B=1, $U^{2(p+1)} = I$ et donc par le lemme 1, la période $k_{A,B}(p)$ divise 2(p+1).
Si $B \neq 1$ dans ce cas il est facile de voir que $U^{2(p+1)\times n} \equiv 1[p]$ si et seulement si n est l'ordre de B^2 (au passage $Ord(B^2) \leq (p-1)/2$ car B d'ordre p-1).
On a donc bien la période $k_{A,B}(p)$ qui divise $2(p-1) \times Ord(B^2)$. Et comme $Ord(B^2) \leq (p-1)/2$ alors $k_{A,B}(p) \leq 2(\text{p-1}) \times Ord(B^2)$. □

7. Algorithme

Résumé. Dans cette partie, nous allons nous focaliser sur un algorithme Maple qui permet de calculer à partir d'un nombre premier les premiers termes de la suite de Fibonacci associés ainsi que sa période. Ce qui va nous permettre d'illustrer les théorèmes 1 et 2 (bornes des périodes). Nous allons commencer par expliquer notre algorithme puis donner des exemples.

7.1. **Déroulement de l'algorithme Maple.**

Les différentes étapes :

1- On fait entrer à l'utilisateur un nombre premier p.

2- On calcule les différents termes de la suite de Fibonacci modulo p.

3- Dès que l'on retombe sur U[n] = 0 et U[n+1] = 1 (avec $n \neq 0$), on arrête le calcul des termes car cela sgnifie que l'on peut déjà extraire la période qui sera ici n (que l'on note k).

4- On vérifie le théorème 1 et 2. On regarde si p est congru à 2 ou 3 modulo 5 (cas 1) ou si il est congru à 1 ou 4 (cas 2).

5- Selon le cas 1 ou 2, on va diviser p-1 ou 2(p+1) par k.

6- Si le résultat de la division est bien un entier alors on a bien démontrer que k divise p-1 ou 2(p+1).

7- On peut aussi vérifier selon les cas que la période est bien inférieur à p-1 ou 2(p+1).

Ce qui nous donne une fois codé en Maple :

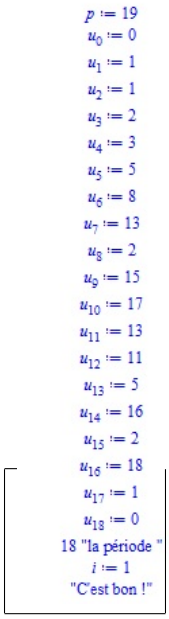
```
with(LinearAlgebra) ;

p := 17 ;
u[0] := 0 ;
u[1] := 1 ;
for n from 2 to p^2 -1 do
u[n] := (u[n-1]+u[n-2]) mod (p) ;
if u[n] = 0 and u[n+1] = 1 then k := n ;
break ;
end if ;
end do ;
"la période "*k ;
l := p mod(5) ;
if l = 1 or l = 4 then
i := (p-1)/k
end if ;
if l = 2 or l = 3 then
i := (2*p+2)/k
end if ;
if type(i, integer) = true then "C'est bon !" else "Pas bon !" end if ;
```

Ici, nous avons choisi de prendre 17 comme nombre premier.

7.2. **Quelques exemples.**

Nous allons maintenant présenter différents exemples avec des nombres premiers.
Pour P = 19



On peut voir ici que la période est de 18. 19 est congru à 4 modulo 5, on a bien ici (p-1)|k, c'est-à-dire (19-1)|18

Pour P = 17

$$
\begin{aligned}
u_{16} &:= 1 \\
u_{17} &:= 16 \\
u_{18} &:= 0 \\
u_{19} &:= 16 \\
u_{20} &:= 16 \\
u_{21} &:= 15 \\
u_{22} &:= 14 \\
u_{23} &:= 12 \\
u_{24} &:= 9 \\
u_{25} &:= 4 \\
u_{26} &:= 13 \\
u_{27} &:= 0 \\
u_{28} &:= 13 \\
u_{29} &:= 13 \\
u_{30} &:= 9 \\
u_{31} &:= 5 \\
u_{32} &:= 14 \\
u_{33} &:= 2 \\
u_{34} &:= 16 \\
u_{35} &:= 1 \\
u_{36} &:= 0
\end{aligned}
$$

On peut voir ici que la période est de 36. 17 est congru à 2 modulo 5, on a bien ici 2(p+2)|k, c'est-à-dire 2(17+2)|36.

Remarque 1. *Il a noté aussi que dans ce cas la période est inférieur ou égale à 2(p+2), ici elle est égale (k = 36), donc on peut dire que dans le cas où p = 17, la période est maximale.*

Autres exemples avec des nombres premiers grands :

Pour P = 701

$u_{681} := 676$
$u_{682} := 220$
$u_{683} := 195$
$u_{684} := 415$
$u_{685} := 610$
$u_{686} := 324$
$u_{687} := 233$
$u_{688} := 557$
$u_{689} := 89$
$u_{690} := 646$
$u_{691} := 34$
$u_{692} := 680$
$u_{693} := 13$
$u_{694} := 693$
$u_{695} := 5$
$u_{696} := 698$
$u_{697} := 2$
$u_{698} := 700$
$u_{699} := 1$
$u_{700} := 0$
700 "la période"

701 est congru à 1 modulo 5 et on a une période k qui est égal à 700 qui divise bien p -1 (701-1).

8. Conclusion

Au travers de ces démonstrations et exemples, nous nous sommes penchés sur l'étude d'une suite récurrente linéaire d'ordre 2 particulière : la suite de Fibonacci. Nous avons pû retrouver des résultats bien connus quand à la périodicité des restes de ses éléments modulo un nombre premier.
Nous avons prouvés que si p est congru à (2 ou 3) mod(5) alors la période de la suite divise $2(p+1)$ ainsi que si p est congru à (1 ou 4) mod(5) alors la période de la suite est de $(p-1)$. L'étude de la matière de Corps Finis nous a permis d'avoir un bagage solide afin de pouvoir traiter et comprendre les théorèmes et subtilitées calculatoires rencontrées.

Ce sujet possède bien des applications intéressantes notemment en cryptologie dans la génération de nombres pseudo-aléatoires, grâce aux registres à décalage à rétroaction linéaire (Linear Feedback Shift Registers en englais, avec pour acronyme LFSR, que nous garderons comme nom par la suite dans un soucis de concision).

Un LFSR est un outil ou logiciel électronique produisant une suite de bits et régie par une fonction mathématique pouvant être vue comme une simple définition de suite récurrente linéaire. On se sert par exemple des n premiers restes modulos 2 des n premiers éléments d'une suite récurrente linéaire donnée, et on applique à un certain nombre de ces restes une opération XOR (appelé aussi "OU exclusif", qui correspond à un simple addition dans le corps F_2). Le résultat obtenu est ensuite concaténé à la suite de bits et on recommence la boucle d'opérations XOR.
Cette notion de LFSR a été généralisée à tout corps fini. Ces LFSR produisent alors des suites de nombres pseudo-aléatoires, et la sécurité de l'ensemble du dispositif repose en partie sur la grande taille de la période de la suite récurrente linéaire assosicée.
Ils restent encore aujourd'hui des générateurs de nombres pseudo-aléatoires très utilisés, en raison de leur faible coût de prodution et d'utilisation. Les nombres pseudo-aléatoires obtenus sont notemment utilisés dans le chiffrement de flux, un des deux principaux moyens de chiffrements actuels en terme d'algorithmes de cryptographie symétrique.

Références

[1] Sanjai Gupta, Parousia Rockstroh, Francis Edwars Su, *Splitting Fields And Periods of Finonacci Sequences Modulo Primes.*

[2] François Arnault, *Arithmétique pour la Cryptographie*, Université de Limoges, Laboratoire d'Arithmétique et d'optimisation.

[3] Abdelkader Necer, *Corps finis Master I Mathématiques.*, Université de Limoges

(Faculté des Sciences et Techniques)
123 Avenue Albert Thomas 87100 Limoges