International Mathematical Forum, Vol. 7, 2012, no. 36, 1793 - 1798

# Une Propriete Arithmetique des Suites Recurrentes Lineaires D'Ordre Trois

**Oumar Fall[1], Oumar Diankha[2], Maurice Mignotte[3] and Mamadou Sangharé[4]**

**Abstract**. The periodicity of LRS modulo $p$, with $p$ a prime integer, was enough studied and it was particularly approached by L. Cerlienco, M. Mignotte and F. Piras in [1].

O. Diankha provided in [2] results, in favour of sequences of the third degree, based on characteristic polynomial. We'll give a arithmetical interpretation of these results, which appear very simple to study the periodicity of LRS of the third degree.

**Résumé**. La périodicité des SRL modulo $p$, oú $p$ est un entier premier, a été beaucoup étudiée et elle a été abordée en particulier par L. Cerlienco, M. Mignotte et F. Piras dans [1].

O. Diankha a fourni dans [2] des résultats, pour les suites d'ordre trois, basés sur le polynôme caractéristique. Nous donnerons une interprétation arithmétique de ces résultats, qui semble être plus simple pour étudier la périodicité d'une SRL d'ordre trois.

**Mots clés:**. Suites Récurrentes linéaires, période, modulo p, polynômes, symboles de Legendre, polynôme caractéristique

## 1. Préliminaires

### 1.2. Formules du discriminant d'un polynome.

[1]Département de Mathématique et Informatique Université Cheikh Anta Diop de Dakar-Sénégal,oumarfall0401@yahoo.fr

[2]Département de Mathématique et Informatique Université Cheikh Anta Diop de Dakar-Sénégal,odiankha@ucad.sn

[3]Département de Mathématique Université Louis Pasteur de Strasbourg-France,maurice.mignotte@math.unistra.fr

[4]Département de Mathématique et Informatique Université Cheikh Anta Diop de Dakar-Sénégal,mamsanghare@hotmail.com

Soit $f(x) \in K[X]$ donné par

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \quad a_0 \neq 0.$$

Par définition, le discriminant de $f$ noté $D(f)$ est

$$D(f) = a_0^{2n-2} \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2$$

si $f(x) = a_0(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ dans une extension convenable du corps $K$. Et on a aussi la formule,

$$D(f) = (-1)^{\frac{n(n-1)}{2}}(a_0)^{-1}R(f,f'),$$

où $R(f,f')$ est le résultant de $f$ et de sa dérivée $f'$.

On peut donner deux lemmes sur le discriminant :

**Lemme 1.** *Si $f$ et $g$ sont deux polynomes unitaires ? coefficients dans un corps, alors leur discriminant vérifie la formule*

$$D(fg) = \pm \operatorname{Res}^2(f,g) \cdot D(f) \cdot D(g).$$

**Preuve.** On a

$$\begin{aligned} D(fg) &= \pm \operatorname{Res}(fg,(fg)') = \pm \operatorname{Res}(fg, fg' + f'g) \\ &= \pm \operatorname{Res}(f, fg' + f'g) \cdot \operatorname{Res}(g, fg' + f'g) \\ &= \pm \operatorname{Res}(f, f'g) \cdot \operatorname{Res}(g, fg') \\ &= \pm \operatorname{Res}(f,f') \cdot \operatorname{Res}(f,g) \cdot \operatorname{Res}(g,f)(g,g'), \end{aligned}$$

d'oú le résultat.

**Lemme 2.** *Si $Q = (X-a)R$ est un polynome cubique ? coefficients dans un corps $K$ de caractéristique différente de deux, avec $R$ irréducitble sur $K$ et $a \in K$, alors le discriminant $\Delta$ de $Q$ n'est pas un carré dans le corps $K$.*

En effet, si $\beta$ et $\gamma$ sont les racines de $R$ dans une extension convenable du corps $K$ alors

$$\Delta = (a-\beta)^2(a-\gamma)^2(\beta-\gamma)^2 = R^2(a)D(R)$$

et $D(R)$ n'est pas un carré dans $K$ (sinon $R$ serait réductible).

**Proposition 1.** *Soit $f(x) \in \mathbb{F}_q[x]$ un polynôme irréductible de degré $d$. Si $\alpha$ est une racine de $f(x)$ dans $\mathbb{F}_{q^d}$, alors toutes les racines de $f$ sont données par $\alpha$, $\alpha^q$, $\alpha^{q^2}$, $\ldots$, $\alpha^{q^{d-1}}$. De plus, $d$ est le plus petit entier positif tel que $\alpha^{q^d} = \alpha$.*

**Preuve.** Voir [3].

**1.2. Suites d'ordre deux**

On considère $\xi$ une suite vérifiant la relation: $\xi_{n+2} = a\xi_{n+1} + b\xi_n$, $n \geq 0$, oú $a, b \in \mathbb{F}_p$ avec $a \neq 0$. On notera, $\Delta = D(f) = a^2 + 4b$.

Les résultats ci-desssous sont bien connus et démontrés en [1].

**Proposition 2.** *On a*
*(i) si* $\left(\frac{\Delta}{p}\right) = 1$, *alors* $t_p$ *divise* $p-1$;
*(ii) si* $\Delta \equiv 0$ *mod* $p$, *alors* $t_p$ *divise* $p(p-1)$;
*(iii) si* $\left(\frac{\Delta}{p}\right) = -1$, *alors* $t_p$ *divise* $p^2-1$.

**Remarque** : La relation (iii) peut être améliorée en

(iii)′: si $\left(\frac{\Delta}{p}\right) = -1$, alors $t_p$ divise le produit $e(p+1)$, oú $e$ est l'ordre de $-b$ dans le corps $\mathbb{F}_p$.

**Proposition 3.** *Pour la suite de Fibonacci définie par* $F_0 = 0$, $F_1 = 1$ *et* $F_{n+2} = F_{n+1} + F_n$ *pour* $n \geq 0$, *on a* $\Delta = 5$ *et*
- *si* $p = 5k \pm 1$, *alors* $t_p$ *divise* $p-1$;
- *si* $p = 5k \pm 2$, *alors* $t_p$ *divise* $2(p+1)$;
- *si* $p = 5$, *alors* $t_p = 20$.

**Remarque :** En appliquant la loi de réciprocité quadratique, on voit que

$$\left(\frac{5}{p}\right) = 1 \iff \left(\frac{p}{5}\right) = 1 \iff p \equiv \pm 1 \pmod 5,$$

ce qui explique le résultat ci-dessus.

**Proposition 4.** *Soit* $(T_n)$ *une SRL de polynôme caractéristique égal ?* $Q(x) = x^3 - ax^2 - bx - c \in \mathbb{Z}[x]$. *Si* $Q$ *est irréductible,* $K \neq K'$, *et* $T_n = \lambda\alpha^n + \mu\beta^n + \nu\gamma^n$, *alors* $t_p$ *divise* $e(p^2+p+1)$, *oú* $e$ *est l'ordre de* $-c$ *dans le corps* $\mathbb{F}_{p^3}$.

**Preuve:** ▷ Puisque $Q(\alpha) = 0$, on a $\alpha^3 - a\alpha^2 - b\alpha - c = 0$. Par cons?quent

$$\begin{aligned} Q(\alpha^p) &= (\alpha^p)^3 - a(\alpha^p)^2 - b\alpha^p - c \\ &= (\alpha^3)^p - a(\alpha^2)^p - b\alpha^p - c \\ &= (\alpha^3)^p - a^p(\alpha^2)^p - b^p\alpha^p - c^p \\ &= (\alpha^3 - a\alpha^2 - b\alpha - c)^p = \big(Q(\alpha)\big)^p = 0. \end{aligned}$$

Donc $\alpha^p = \alpha$ ou $\beta$ ou $\gamma$. Or $x^p = x \Leftrightarrow x \in K$, puisque $\alpha \notin K$, alors $\alpha^p = \beta$ ou $\gamma$. Si $\alpha^p = \beta$, alors $Q(\beta) = 0 = \beta^3 - a\beta^2 - b\beta - c$. Alors:

$$\begin{aligned} (\beta^3 - a\beta^2 - b\beta - c)^p = 0 &= (\beta^p)^3 - a^p(\beta^p)^2 - b^p\beta^p - c^p \\ &= (\beta^p)^3 - a(\beta^p)^2 - b\beta^p - c = Q(\beta^p). \end{aligned}$$

Donc $\beta^p = \gamma = (\alpha^p)^p = \alpha^{p^2}$.

On a aussi

$$\alpha\beta\gamma = -c = \alpha\alpha^p\alpha^{p^2} = \alpha^{1+p+p^2}.$$

Soit $e$ l'ordre de $-c$ dans $K' = \mathbb{F}_{p^3}$. Donc $(\alpha\beta\gamma)^e = \alpha^{e(1+p+p^2)} = (-c)^e = 1$. Et puisque $t_p =$ ordre de $\alpha$, on voit que $t_p$ divise le produit $e(1+p+p^2)$. ◁

**Proposition 5.** *Pour la suite de Fibonacci d'ordre* 3, *si* $Q$ *est irréductible et* $K \neq K'$ *et aussi* $T_n = \lambda\alpha^n + \mu\beta^n + \nu\gamma^n$, *alors* $t_p$ *divise* $2(p^2+p+1)$.

**Remarque :** L'entier $2(p^2+p+1)$ est plus petit que $p^3-1$ pour $p \geq 3$, ce qui permet d'améliorer donc la borne générale $p^3-1$.

| $p$ | $t_p$ | $p^3-1$ | $2(1+p+p^2)$ |
|---|---|---|---|
| 2 | 7 | 7 | 14 |
| 3 | 13 | 26 | 26 |
| 13 | 183 | 2196 | 366 |
| 29 | 871 | 24388 | 1742 |
| 31 | 993 | 29790 | 1986 |
| 41 | 1723 | 68920 | 3446 |
| 47 | 2257 | 103822 | 4514 |
| 71 | 5113 | 357910 | 10226 |
| 73 | 5403 | 389016 | 10806 |
| 127 | 16257 | 2048382 | 32514 |
| 131 | 17293 | 2248090 | 34586 |
| 139 | 19461 | 2685618 | 38922 |
| 151 | 1093 | 3442950 | 45906 |
| 163 | 8911 | 4330746 | 53466 |
| 179 | 32221 | 5735338 | 64442 |
| 193 | 37443 | 7189056 | 74886 |

**Remarque:** E. Kern et M. Mignotte ont donné, dans [5], ce résultat proche de la proposition 6 de l'étude arithmétique.

Soit $P = X^d + a_1X^{d-1} + \cdots + a_d \in K[X] = \mathbb{Q}[\mathbb{X}]$ un polynôme unitaire et irréductible de matrice compagnon $A$ d'ordre $k$. On suppose que $P$ se d?compose modulo $p$ en $\widetilde{P} = P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r}$, $e_1$, $e_2$, ... , $e_r \geq 1$, où les $P_i \in \mathbb{F}_p[X]$ sont unitaires irréductibles et deux à deux distincts. Alors

$$\mathbb{F}_p[A] \sim \frac{\prod_{i=1}^{i=r}\mathbb{F}_p[X]}{(P_i^{e_i})}.$$

$\widetilde{P} = P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r} \Leftrightarrow (p) = P_1^{e_1}P_2^{e_2}\cdots P_r^{e_r}$ de l'idéal $(p)$ dans le corps de rupture de $P$, $\frac{K[X]}{(p)}$ et le degré résiduel de $P_i$ est $f_i$ (résultat dû à Kummer).

Pour $d = 3$, on a les possibilités suivantes:

- $k \mid p-1$, alors $(p) = P_1P_2P_3$, avec des $P_i$ distincts et $f_1 = f_2 = f_3 = 1$.
- $k \mid p(p-1)$ et $k \not\mid p-1$, alors $(p) = P_1^2P_2$, avec $P_1 = P_2$ ou $P_1 \neq P_2$ et $f_1 = f_2 = 1$.
- $k \mid p^2-1$ et $k \not\mid p-1$, alors $(p) = P_1P_2$, avec $f_1 = 2$ et $f_2 = 1$.
- $k \mid p^3-1$ et $k \not\mid p-1$, alors $(p) = P_1$, avec $f_1 = 3$.

Nous proposons l'approche suivante:

**2. Etude arithmétique**

**Proposition 6.** *Soit $(T_n)$ une SRL d'ordre trois, de polynôme caractéristique $Q(x) = x^3 - ax^2 - bx - c \in \mathbb{Z}[x]$. Soit $\Delta$ son discriminant, et soit $p$ un entier premier et $t_p$ la période de la suite modulo $p$. Alors on a les quatre cas suivants :*

- *si $\Delta \equiv 0 \pmod p$, alors $t_p$ divise $p(p-1)$ ;*
- *si $\left(\frac{\Delta}{p}\right) = -1$, alors $t_p$ divise $p^2 - 1$ ;*
- *si $\left(\frac{\Delta}{p}\right) = 1$ et $Q$ admet au moins une racine modulo $p$, alors $t_p$ divise $p - 1$ ;*
- *si $\left(\frac{\Delta}{p}\right) = 1$, avec $Q$ irréductible modulo $p$, alors $t_p$ divise $p^3 - 1$ .*

**Remarque:** Cette dernière relation peut être améliorée. En effet, d'après la proposition 4, si $\left(\frac{\Delta}{p}\right) = 1$, avec $Q$ irréductible, alors $t_p$ divise $e(p^2 + p + 1)$ .

**Preuve :** ▷ • Le cas $\Delta \equiv 0 \pmod p$ est clair.

• Supposons que $Q(X) = (X - a)R(X)$.

D'après le lemme 2, cela équivaut à :

$$\Delta = (a-\beta)^2(a-\gamma)^2(\beta-\gamma)^2 = R^2(a)D(R),$$

ou encore ? $\left(\frac{\Delta}{p}\right) = -1$ puisque $D(R)$ n'est pas un carré dans $K$ (sinon le facteur $R$ serait réductible). Donc $t_p$ divise $p^2 - 1$.

• Supposons que $Q(X) = (X-\alpha)(X-\beta)(X-\gamma)$ dans $\mathbb{F}_p[X]$, alors

$$\Delta = (\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2 = R^2(a)D(R)$$

(avec $R(X) = (X-\beta)(X-\gamma)$), ce qui ?quivaut encore ? $\left(\frac{\Delta}{p}\right) = 1$ car $R$ est réductible. Et donc $t_p$ divise $p - 1$.

• Supposons que $R$ est irréductible, alors

$$\begin{aligned}\Delta &= (\alpha-\alpha^p)^2(\alpha-\alpha^{p^2})^2(\alpha^p-\alpha^{p^2})^2 \\ &= (\alpha^{p+2} - \alpha^{p^2+2} + \alpha^{2p^2+1} - \alpha^{2p+1} + \alpha^{p^2+2p} - \alpha^{2p^2+p})^2.\end{aligned}$$

Posons $\gamma = \alpha^{p+2} - \alpha^{p^2+2} + \alpha^{2p^2+1} - \alpha^{2p+1} + \alpha^{p^2+2p} - \alpha^{2p^2+p}$. Alors

$$\gamma^p = \alpha^{p^2+2p} - \alpha^{1+2p} + \alpha^{2+p} - \alpha^{2p^2+p} + \alpha^{1+2p^2} - \alpha^{2+p^2} = \gamma.$$

Donc $\gamma \in K$ et $\Delta = \gamma^2$. D'où : $\left(\frac{\Delta}{p}\right) = 1$.

Exemples : Suite de Fibonacci d'ordre 3. Il s'agit de la suite $(T_n)$ à valeurs dans $\mathbb{Z}$ définie par $T_0 = T_1 = 0$, $T_2 = 1$ et $T_{n+3} = T_{n+1} + T_n$ pour tout

$n \geq 0$. Son polynôme caractéristique est $Q(x) = x^3 - x - 1$ et son discriminant vaut $\Delta = -23$.

1) pour $p = 23$; $\Delta \equiv 0 \pmod{23}$ et on a $t_p = 506 = 23 \times 22$,

2)

| $p$ | 5 | 7 | 11 | 17 | 19 | 37 | 43 | 53 | 61 | 67 | 79 | 83 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $t_p$ | 24 | 48 | 120 | 288 | 180 | 1368 | 231 | 1404 | 930 | 4488 | 3120 | 2296 |

| $p$ | 89 | 97 | 103 | 107 | 109 | 113 | 137 | 149 | 157 | 181 | 191 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $t_p$ | 3960 | 3136 | 3536 | 2862 | 1485 | 4256 | 391 | 925 | 12324 | 10920 | 7296 |

Pour chaque entier $p$, on a : $\left(\frac{-23}{p}\right) = -1$ et donc $t_p$ divise $p^2 - 1$.

3)

| $p$ | 2 | 3 | 13 | 29 | 31 | 41 | 47 | 71 |
|---|---|---|---|---|---|---|---|---|
| $t_p$ | 7 | 13 | 183 | 871 | 993 | 1723 | 2257 | 5113 |

| $p$ | 73 | 127 | 131 | 139 | 151 | 163 | 179 | 193 |
|---|---|---|---|---|---|---|---|---|
| $t_p$ | 5403 | 16257 | 17293 | 19461 | 1093 | 8911 | 32221 | 37443 |

Pour chaque entier $p$, $\left(\frac{-23}{p}\right) = 1$ et $Q$ est irréductible. Alors $t_p$ divise $p^3 - 1$.

4)

| $p$ | 59 | 101 | 167 | 173 |
|---|---|---|---|---|
| $t_p$ | 58 | 100 | 166 | 172 |

Pour chaque entier $p$, $\left(\frac{-23}{p}\right) = 1$ et $Q$ est réductible. Alors $t_p$ divise $p - 1$.

# References


[1] **L. Cerlienco, M. Mignotte, F. Piras**, Suites Récurrentes linéaires. Propriétés Algébriques et Arithmétiques. L'Enseignement mathématique, t.33(1987), p.67-108. A.M.S. Classification: 10 A 35.

[2] **O. Diankha**, Suites récurrences linéaires sur un corps fini. Théorie et Applications, Afrika Matematica, série 3, Volume 18 2007, pp.46-60.

[3] **R. Lidl, H. Niederreiter**, Introduction to finite fields and their applications, Cambridge University Press 1994.

[4] **M. Mignotte**, Mathematics for Computer Algebra. 1992 Springer-Verlag, New York, Inc.

[5] **E. Kern, M. Mignotte**, Applications of the representation of finite fields by matrices. Theoretical Computer Science 244(2000) 263-265.


**Received: November, 2011**