Séminaire Delange-Pisot-Poitou. Théorie des nombres

Marcel Duboué

Une suite récurrente remarquable

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 19, n° 2 (1977-1978), exp. n° 27, p. 1-12

<http://www.numdam.org/item?id=SDPP_1977-1978__19_2_A3_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
19e année, 1977/78, n° 27, 12 p.

6 février 1978

UNE SUITE RÉCURRENTE REMARQUABLE

par Marcel DUBOUÉ

Soit ξ , racine du polynôme monique irréductible $P(x)$ de discriminant Δ_1 . Soit K le corps $\mathbb{Q}(\xi)$ de discriminant Δ . On a $\Delta_1 = q_1^2 \Delta$.

D'autre part, ξ^n est racine d'un polynôme monique, non nécessairement irréductible, $P_n(x)$ de discriminant $\Delta_n = q_n^2 \Delta$, et de même degré r que $P(x)$. On a alors $q_n = q_1 F_n$.

Nous montrons que la suite (F_n) est une suite récurrente d'ordre factorielle de r , et que la loi d'apparition des zéros dans la suite (F_n modulo p), p premier, reflète la structure de décomposition de l'idéal (p) dans le corps K .

Ces propriétés généralisent celles, classiques, des nombres de Fibonacci étudiés par LUCAS qui correspondent au cas $r = 2$.

Les propriétés arithmétiques des suites d'entiers $(F_n , n \in \mathbb{N})$, définies par une récurrence linéaire de second ordre, sont le sujet d'une littérature abondante dominée par les travaux classiques de E. LUCAS au sujet des nombres de Fibonacci.

Les résultats essentiels étaient :

(L1) $F_n = \dfrac{\alpha^n - \beta^n}{\alpha - \beta}$ α , β racines de $x^2 - ax - b = P(x) = 0$;

(L2) $m \mid n \Longrightarrow F_m \mid F_n$;

(L3) $s = \left(\dfrac{\Delta}{P}\right) \Longrightarrow F_p \equiv s , \ F_{p-s} \equiv 0 \pmod p$, Δ discriminant de $P(x)$.

La loi (L3) explicite le comportement de la suite (F_n) modulo p . LUCAS justifiait ce genre de préoccupation dans [8] : "La théorie des suites récurrentes est une mine inépuisable qui renferme toutes les propriétés des nombres. En calculant les termes successifs de telles suites, en décomposant ceux-ci en facteurs, en recherchant par l'expérimentation les lois de l'apparition et de la reproduction des nombres premiers, on fera progresser d'une manière systématique l'étude des propriétés des nombres et de leurs applications dans toutes les branches des mathématiques."

Divers auteurs, et en particulier M. WARD, G. E. ANDREWS ont cherché à généraliser cette théorie aux récurrences linéaires d'ordre supérieur.

Nous proposons ici une approche différente en étudiant des nombres liés aux discriminants de polynômes dont l'étude a été suggérée par R. D. CARMICHAEL [3], et dans un cadre conceptuel imaginé par M. P. SCHÜTZENBERGER et P. BARRUCAND.

Posons pour abréger

$$\varphi_n(x\ ,\ y) = \Sigma\{x^j\ y^{n-1-j}\ ,\ \ 0 \leqslant j \leqslant n-1\}\ ,\ (= \frac{x^n - y^n}{x - y})\ .$$

Un polynôme monique $P(x)$ étant donné, nous définissons, quel que soit n

$$F_n(P) = F_n = \prod \varphi_n(\alpha\ ,\ \beta)$$

où le produit est étendu à toutes les paires de racines de $P(x) = 0$.

Si $P(x)$ n'a pas de racine multiple, c'est bien le rapport $\sqrt{\Delta_n}/\sqrt{\Delta_1} = q_n/q_1$ évoqué dans le préambule.

Dans le cas où $P(x)$ est du second degré, on retrouve la définition (loi (L1) de Lucas) des nombres de Fibonacci. De nombreuses propriétés des F_n , et en particulier la divisibilité, sont de nature purement algébrique, aussi nous les établirons dans la première partie en considérant, à la place des α_i racines d'un polynôme, des variables formelles x_i .

Nous montrerons que les F_n (alors dénotés Φ_n) sont certaines fonctions symétriques remarquables. Nous établirons que leur fonction génératrice

$$\mathfrak{F}(t) = \sum_{0 \leqslant n} \Phi_{n+1}\ t^n$$

est rationnelle, et nous en déduirons que les Φ_n satisfont une récurrence linéaire d'ordre factorielle de $\underset{\sim}{r}$, où $\underset{\sim}{r}$ est le nombre de variables (versus le degré du polynôme $P(r)$).

Dans la seconde partie, purement arithmétique, nous étudierons l'apparition et la reproduction des nombres premiers dans les suites (F_n) , et nous montrerons qu'en fait les lois de Lucas et leur extension aux ordres supérieurs traduisent la structure des idéaux dans l'extension algébrique de $\underset{\sim}{Z}$ par une racine de $P(x) = 0$.

Dans la troisième partie, nous traiterons en détail les cas quadratique et cubique, et nous en déduirons une méthode pratique pour trouver la structure d'un idéal (p) dans un corps cubique quelconque.

Concepts utilisés.

Dans la première partie : Fonctions symétriques, fonctions de Schur, déterminant de Vandermonde, série génératrice.

Dans la deuxième partie : Corps de Galois, théorème de Zolotarev, décomposition des idéaux.

Première partie : propriétés algébriques.

1. Définitions.

Soient x , y des variables formelles, et X , Y des ensembles finis de telles variables.

$$\varphi_n(x\ ,\ y) = \sum_{0 \leqslant j \leqslant n-1} x^j\ y^{n-1-j}\ ,\ \ (= \frac{x^n - y^n}{x - y})\ ,\ \ n \geqslant 1\ .$$

$$\Psi_n(X , Y) = \prod\{\varphi_n(x , y) ; \quad x \in X , \quad y \in Y\} .$$

$$\Phi_n(X) = \prod\{\varphi_n(x , y) ; \quad \{x , y\} \in X \times X\} .$$

$$\Phi_n(X) = 1 \quad \text{si} \quad \|X\| = 1 .$$

2. Propriétés de divisibilité.

(1) $$\varphi_{md}(x , y) = \varphi_m(x , y)\ \varphi_d(x^m , y^m)$$

car

$$\frac{x^{md} - y^{md}}{x - y} = \frac{x^m - y^m}{x - y} \cdot \frac{x^{md} - y^{md}}{x^m - y^m}$$

D'où les propriétés analogues pour les polynômes Φ_n et Ψ_n par simple passage au produit. Notons $X^{(m)} = \{x^m ; \ x \in X\}$.

(2) $$\Psi_{md}(X , Y) = \Psi_m(X , Y)\ \Psi_d(X^{(m)} , Y^{(m)}) .$$

(3) $$\Phi_{md}(X) = \Phi_m(X)\ \Phi_d(X^{(m)}) .$$

D'où,

(4) $$m|n \Longrightarrow \Phi_m | \Phi_n ,$$

les polynômes Φ_n constituent une séquence de divisibilité.

3. Propriétés de symétrie.

On a par définition $\varphi_n(x , y) = \varphi_n(y , x)$, donc $\Psi_n(X , Y) = \Psi_n(Y , X)$, et $\Phi_n(X)$ est un polynôme symétrique en les variables $x_i \in X$.
De plus, $\Phi_n(X) = \prod_{1 \leq i < j \leq r}((x_i^n - x_j^n)/(x_i - x_j))$, si $\|X\| = r$.

$$\Phi_n(X) = \frac{\prod_{i,j}(x_i^n - x_j^n)}{\prod_{i,j}(x_i - x_j)} = \frac{\Delta(X^{(m)})}{\Delta(X)} = \frac{\Delta_n}{\Delta_1}$$

où $\Delta(X)$ est le déterminant de Vandermonde des variables x_i . Donc

(5) $\Phi_n(X)$ est la fonction de Schur associée à la partition

$$\{(n - 1) , 2(n - 1) , \ldots , (r - 2)(n - 1) , (r - 1)(n - 1)\} .$$

4. Fonction génératrice et récurrence des $\Phi_n(X)$.

Soit $\mathfrak{F}(t) = \sum_{n \geq 0} \Phi_{n+1}\ t^n$, la série génératrice des $\Phi_n(X)$.
D'après ce qui précède :

$$\mathfrak{F}(t) = \sum_{n \geq 0} \frac{\Delta_{n+1}}{\Delta_1}\ t^n = \frac{1}{\Delta_1} \sum_{n \geq 0} \Delta_{n+1}\ t^n = \frac{1}{\Delta_1} \sum_{n \geq 0}\ t^n \Big(\sum_{\sigma \in \mathfrak{S}_r} (-1)^\sigma\ \xi_\sigma^{n+1}\Big) ,$$

où $\xi_\sigma = \prod_{i \in [r]} x_{\sigma(i)}^{(r-i)}$

$$\mathfrak{F}(t) = \frac{1}{\Delta_1} \sum_{\sigma \in \mathfrak{S}_r} (-1)^\sigma \sum_{n \geq 0} \xi_\sigma^{n+1}\ t^n = \frac{1}{\Delta_1} \sum_{\sigma \in \mathfrak{S}_r} \frac{(-1)^\sigma\ \xi_\sigma}{1 - \xi_\sigma\ t} .$$

On sait, par les propriétés des déterminants de Vandermonde, que le terme Δ_1 se

simplifie, donc nous avons le théorème suivant.

THÉORÈME 1. - La série génératrice des $\Phi_n(X)$ est une fonction rationnelle, symétrique en les variables x_i, dont le dénominateur $R(t) = \prod_{\sigma\in\gamma_r}(1 - \xi_\sigma t)$ est de degré factorielle de r, $r = \|X\|$.

COROLLAIRE. - La suite des polynômes $\Phi_n(X)$ satisfait une relation de récurrence linéaire, d'ordre $r!$. Le polynôme de la récurrence $R^*(t)$ est le polynôme réciproque de $R(t)$ donné au théorème 1.

5. Propriétés liées aux partitions.

Soit $\{X_i \ ; \ 1 \leqslant i \leqslant \ell\}$ une partition de X. On note $X = \sum_{1\leqslant i\leqslant \ell} X_i$. Alors

$$\Psi_n(X , Y) = \prod_{1\leqslant i\leqslant \ell} \Psi_n(X_i , Y) . \tag{6}$$

C'est évident par la définition de Ψ_n.

$$\Phi_n(X) = \prod_{1\leqslant i\leqslant \ell} \Phi_n(X_i) \prod_{1\leqslant i\leqslant \ell} \Psi_n(X_i , X_j) . \tag{7}$$

Deuxième partie : Propriétés arithmétiques.

On donne aux variables x_i des valeurs α_i prises dans un corps $\underset{\sim}{K}$. On notera alors F_n les valeurs de Φ_n, G_n les valeurs de Ψ_n, et f_n les valeurs de φ_n.

La fonction valeur(x_i) n'étant pas nécessairement injective, on doit considérer l'"ensemble" des valeurs α_i comme un ensemble "avec multiplicité", ou $\underset{\sim}{N}$-ensemble au sens d'Eilenberg.

On notera $X^{\#}$ le $\underset{\sim}{N}$-ensemble des valeurs α_i, et X, son support, l'ensemble des valeurs α_i.

On définit la multiplicité μ_i de la valeur α_i par

$$\mu_i = \operatorname{card}\{x_i \ ; \ \text{valeur}(x_i) = \alpha_i\} .$$

Alors, nous avons le théorème suivant.

THEOREME 2. - Si $X^{\#}$ est un $\underset{\sim}{N}$-ensemble de valeurs α_i d'un corps K, α_i étant de multiplicité μ_i, si $k_i = (\mu_i(\mu_i - 1))/2$, $k = \sum_i \mu_i$, alors

$$F_n = n^k \Big(\prod_{\alpha_i\in X} \alpha^{k_i} \Big)^{n-1} \prod_{\{\alpha_i,\alpha_j\}\ X\times X} f_n^{\mu_i\mu_j}(\alpha_i , \alpha_j) .$$

Preuve. - On utilise la formule (7) où la partition X_i est constituée de l'ensemble des x_k qui ont la même valeur α_i.

Alors

$$F_n(X_i) = \prod_{1\leqslant j<k\leqslant \mu_i} f_n(\alpha_i , \alpha_i) = f_n^{k_i}(\alpha_i , \alpha_i) .$$

Or, d'après la définition de φ_n , $\varphi_n(x , x) = nx^{n-1}$, donc $F_n(X_i) = (n\alpha_i^{n-1})^{k_i}$.
Donc

$$\prod_{1\leqslant i\leqslant \ell} F_n(X_i) = n^k(\prod_{1\leqslant i\leqslant \ell} \alpha_i^{k_i})^{n-1} .$$

De plus

$$\Psi_n(X_i , X_j) = \prod_{\substack{1\leqslant h\leqslant \mu_i \\ 1\leqslant k\leqslant \mu_j}} f_m(\alpha_i , \alpha_j) = f_n^{\mu_i\mu_j}(\alpha_i , \alpha_j) .$$

Ce qui achève la démonstration.

6. Définition.

Soit $P(x) = x^r - a_1 x^{r-1} - \ldots - a_r$, un polynôme monique de degré r , à coefficients dans un anneau A , de racines $\alpha_1 , \ldots , \alpha_r$ dans un corps K . On appelle nombres de Schützenberger associés à $P(x)$ la suite

$$F_n(P) = F_n = \Phi_n(\alpha_1 , \ldots , \alpha_r) , \quad n \geqslant 1 , \quad F_n \in A .$$

D'après ce qui précède, cette définition est valide même si $P(x)$ a des racines multiples.
Dans le cas où $P(x)$ n'a pas de racine multiple, le paragraphe 3 montre que les F_n , quotients de deux déterminants, sont une racine carrée du quotient de deux discriminants puisque, par définition, $\Delta(P_n) = \prod(\alpha^n - \beta^n)^2$, où $\{\alpha , \beta\}$ parcourt les paires de racines.
Notre façon d'aborder le problème nous a évité d'avoir à choisir une détermination de cette racine carrée, choix qui n'avait à priori aucune signification.
Les F_n appartiennent à l'anneau de base A , car ce sont des fonctions symétriques des racines de $P(x)$.

7. Propriétés de divisibilité et de récurrence.

Les résultats de la première partie ont pour conséquence immédiate :

(8) $$m|n \Longrightarrow F_m|F_n ,$$

les F_n constituent une séquence de divisibilité. Et, plus précisément, si $P_m(X)$ est le polynôme qui a pour racines les puissances m-ièmes de celles de $P(X)$, alors nous avons :

(9) $$F_{md}(P) = F_m(P)\ F_d(P_m) ,$$

(10) Les nombres de Schützenberger associés à un polynôme de degré r satisfont une récurrence linéaire d'ordre factorielle de r . Le polynôme de récurrence est donné au théorème 1.

8. Etude des nombres de Schützenberger modulo les nombres premiers.

On se propose de poursuivre l'étude arithmétique de ces nombres F_n de façon à généraliser les lois classiques en ce qui concerne le rang d'apparition des nombres premiers comme facteurs des F_n , c'est-à-dire le rang des 0 de la suite

(F_n modulo p).

Si A est un anneau principal, soit $P = P_1^{\mu_1} \dots P_\ell^{\mu_\ell}$, la décomposition irréductible sur A du polynôme monique P en polynômes moniques P_i , et soit ϖ_i le produit des racines de P_i .

Alors

$$(11) \qquad F_n(P) = n^k \Big(\prod_{1\leq i\leq \ell} \varpi_i^{k_i} \Big)^{n-1} \Big(\prod_{1\leq i\leq \ell} F_n^{\mu_i^2}(P_i) \Big) \Big(\prod_{1\leq i<j\leq \ell} G^{\mu_i\mu_j}(P_i , P_j) \Big) .$$

Preuve. - Dans (7), on prend comme partition de X $\{X_i ; 1 \leq i \leq \ell\}$, où X_i est le $\underset{\sim}{N}$-ensemble des racines de $P_i^{\mu_i}$. Toutes les racines dans X_i ont la même multiplicité μ_i , et le théorème 2 fournit le résultat.

Notons que les ϖ_i , F_n , G_n appartiennent à l'anneau A .

Notation. - Lorsqu'on considèrera $A \equiv \underset{\sim}{Z}$, on notera F_n et G_n , $A \equiv \underset{\sim}{Z}_p$, on notera $\bar{F}_n$ et $\bar{G}_n$.

Soit $\bar{P}(x) = P(x) \mod p$ défini par :

- $\bar{P}(x) \in \underset{\sim}{Z}_p[x]$;
- $\bar{P}(x)$ monique ;
- $\bar{P}(x) = \bar{P}(x) + pQ(X)$.

Alors

$$(12) \qquad \bar{F}_n(\bar{P}) = F_n(P) \mod p .$$

En effet, d'après le § 3, $\Phi_n(X)$ est fonction symétrique des x_i , donc $F_n(P)$ est fonction symétrique des racines α_i de P , donc ne dépend que des coefficients a_i de P .

Donc, d'après (11) où l'on prend $\underset{\sim}{Z}_p \equiv A$, nous avons le théorème suivant.

THEOREME 3. - Si $\bar{P}(x) = \prod_{1\leq i\leq \ell} \bar{P}_i^{\mu_i}(x)$, alors $F_n(P) \equiv 0 \mod p$ si, et seulement si, l'une des conditions suivantes est satisfaite :

(i) $p|n$, et $\bar{P}_i$ est facteur multiple de P ;

(ii) $p|a_r$ et $p|a_{r-1}$;

(iii) $\exists\, i$; $\bar{F}_n(\bar{P}_i) = 0$, $n > 1$;

(iv) $\exists\, i , j$; $\bar{G}_n(\bar{P}_i , \bar{P}_j) = 0$.

Preuve.

$$k_i \neq 0 \Longleftrightarrow \mu_i > 1 \Longleftrightarrow \bar{P}_i \text{ est facteur multiple de } P .$$

$$k \neq 0 \Longleftrightarrow \exists\, i ; \ k_i \neq 0 \Longleftrightarrow P \text{ a un facteur multiple.}$$

Alors

(i) vient de la considération du facteur n^k ;

(ii) vient du facteur $\prod_i \varpi_i^{k_i(n-1)}$ qui est nul si, et seulement si, $\exists\, i$; $\varpi_i = 0$, et 0 est racine multiple de $\bar{P}(x) = P(x) \mod p$;

(iii) et (iv) viennent de l'annulation des facteurs F_n et G_n, car μ_i est toujours non nul.

A la lumière du théorème de Zolotarev ([4] page 113...), qui relie la décomposition du polynôme $\bar{P}(x)$ à la décomposition de l'idéal (p) $(p > r)$ dans une extension algébrique de $\underset{\sim}{Z}$ par une racine de $P(x)$, nous allons préciser les conditions du théorème 3 en terme de décomposition de l'idéal (p).

Donc, nous considèrerons dorénavent que $P(x)$ est irréductible sur $A \equiv \underset{\sim}{Z}$.
Montrons, tout de suite, un résultat analogue à la loi L3 de Lucas.

(13) Si $s = (\frac{\Delta}{p})$ alors $P_p \equiv s \mod p$, où Δ est le discriminant de $P(x)$.

Preuve. - Si $\bar{P}(x)$ a des racines multiples, ce qui est équivalent à $s = 0$, alors la condition (ii) du théorème 3 fournit $F_p \equiv 0 \mod p$.
Sinon, $P(x)$ n'a pas non plus de racines multiples et

$$F_p = \prod_{1\leqslant i<j\leqslant r} \frac{\alpha_i^p - \alpha_j^p}{\alpha_i - \alpha_j} \equiv \prod_{1\leqslant i<j\leqslant r} \frac{(\alpha_i - \alpha_j)^p}{\alpha_i - \alpha_j} \mod p$$
$$\equiv \prod_{1\leqslant i<j\leqslant r} (\alpha_i - \alpha_j)^{p-1} \equiv \Delta^{(p-1)/2} = (\frac{\Delta}{p}) .$$

Ce qui achève la démonstration.

9. Rappel de quelques propriétés des corps finis (corps de Galois).

Certaines de ces propriétés sont classiques. Nous les donnons avec nos notations pour la clarté de l'exposé.

9.1. - Si $\bar{P}(x)$ est irréductible sur $\underset{\sim}{Z}_p$, de degré ν, le corps K de ses racines (extension algébrique de $\underset{\sim}{Z}_p$ par adjonction de toutes les racines de $\bar{P}$) est d'ordre p^ν. Son groupe multiplicatif est cyclique, d'ordre $p^\nu - 1$.
Les éléments de K sont toutes les racines de $x^{p^\nu} - x = 0$. Un élément est dit de degré k, s'il est racine d'une équation irréductible de degré k.
On note $GF(p^\nu)$ le corps fini K défini plus haut (Galois Field). Alors, si $\mu | \nu$, $GF(p^\mu) \subseteq GF(p^\nu)$.
Si $\alpha \in GF(p^\nu)$, alors, le degré μ de α divise ν, et $\alpha \in GF(p^\mu)$.

9.2. - Si α est une racine de $\bar{P}(x)$, les autres racines sont

$$\alpha^p , \alpha^{p^2} , \ldots , \alpha^{p(\nu-1)} .$$

La structure de $GF(p^\nu)$ est donc la suivante. Pour tout $\mu | \nu$, $GF(p^\nu)$ contient n_p μ-uplets de racines conjuguées, où n_μ est le nombre de polynômes de degré μ, irréductibles sur $\underset{\sim}{Z}_p$ (en fait, il s'agit de polynômes séparables mais dès que $p > \nu$, qui est le cas qui nous intéresse, c'est la même notion).

9.3. - Soit η_i l'endomorphisme multiplicatif de $GF(p^\nu)$: $x \longmapsto x^i$. Soit $\{\alpha\}_\#$ l'ensemble de tous les conjugués de α.
Alors l'image par η_i d'une classe de conjugués est une classe de conjugués.

$$\forall\ i\ :\ \eta_i(\{\alpha\}_*) = \{\eta_i(\alpha)\}_*\ .$$

En effet, d'après 9.2, $\{\alpha\}_* = \{\alpha^{p^j}\ ;\ j \in [\nu - 1]\}$.

Alors, $\forall\ j$, $(\alpha^i)^{p^j} \equiv (\alpha^{p^j})^i$, d'où le résultat.

9.4. - η_i <u>bijective sur</u> $\{\alpha\}_* \Longleftrightarrow \eta_i(\alpha)$ <u>est de degré</u> ν .

En effet :

$$\begin{aligned}
\eta_i \text{ non bijective sur } \{\alpha\}_* &\Longleftrightarrow \exists\ \alpha' \in \{\alpha\}_*\ ;\ \eta_i(\alpha) = \eta_i(\alpha') \\
&\Longleftrightarrow \exists\ j < \nu\ ;\ \eta_i(\alpha) = \eta_i(\alpha^{p^j}) \text{ , d'après 9.2} \\
&\Longleftrightarrow \exists\ j < \nu\ ;\ (\alpha^i) = (\alpha^i)^{p^j} \\
&\Longleftrightarrow \exists\ j < \nu\ ;\ \eta_i(\alpha) \in GF(p^j) \text{ , d'après 9.1.}
\end{aligned}$$

D'où le résultat en prenant la négation des deux termes de l'équivalence, compte tenu de $\eta_i(\alpha)$ de degré ν si, et seulement si, $\eta_i(\alpha) \in GF(p^\nu)$, et, $\forall\ j < \nu$, $\eta_i(\alpha) \notin GF(p^j)$.

9.5. - <u>Si</u> $\mu | \nu$, $\mu \neq \nu$, <u>alors</u> $\eta_{(p^\nu-1)/(p^\mu-1)}$ <u>n'est bijective sur aucune classe</u> $\{\alpha\}_*$.

En effet, d'après la structure cyclique de $GF(p^\nu)$ et de ses sous-groupes, on a évidemment $\eta_{(p^\nu-1)/(p^\mu-1)}(\alpha) \in GF(p^\mu)$, quel que soit α .

9.6. - η_i <u>est un automorphisme de</u> $GF(p^\nu) \Longleftrightarrow (i\ ,\ p^\nu - 1) = 1$.

Soit ξ une racine primitive de $GF(p^\nu)$. D'après 9.1, tous les éléments non nuls de $GF(p^\nu)$ sont $\{\xi^j\ ;\ j \in [p^\nu - 1]\}$. Alors

$$\eta_i(\xi^j) = \eta_i(\xi^k) \Longleftrightarrow \eta_i(\xi^{j-k}) = 1\ ,\quad j > k\ .$$

Si $(i\ ,\ p^\nu - 1) = 1$, alors ξ^i est aussi racine primitive, et

$$\eta_i(\xi^{j-k}) = (\xi^i)^{j-k}\ .$$

Donc $j = k$, et η_i est bijective.

Si $(i\ ,\ p^\nu - 1) = d \neq 1$, alors, d'après la structure cyclique du groupe multiplicatif de $GF(p^\nu)$, η_d n'est pas bijective car $d | p^\nu - 1$, donc η_i non plus car $d | i$.

Compte tenu de $(p^i\ ,\ p^\nu - 1) = 1$, on retrouve ainsi les classiques η_{p^i} , automorphismes de Frobénius qui, d'après 9.2, sont aussi des automorphismes des classes de conjugués.

10. <u>Résolution des conditions du théorème</u> 3.

10.1. - <u>Si</u> (p) <u>est ramifié (ou pseudo-ramifié), alors</u> $F_p \equiv 0 \mod p$.

Cette condition exprime (i) en terme d'idéal.

10.2. - <u>Pour</u> $p > r$, <u>si</u> (p) <u>possède</u> $(k + 1)$ <u>facteurs linéaires distincts</u>, $k \geqslant 1$, $k | p - 1$, <u>alors</u> $F_{(p-1)/k} \equiv 0 \mod p$.

Soient α et β deux racines rationnelles de $\bar{P}(x) = 0$.

$$\alpha^n = \beta^n \Longleftrightarrow (\alpha\beta^{-1})^n = 1$$
$$\Longleftrightarrow \exists\, k \ ; \ (\alpha\beta^{-1})^{(p-1)/k} = 1 \Longleftrightarrow \exists\, k \ ; \ \alpha^{(p-1)/k} = \beta^{(p-1)/k} ,$$

ce qui est équivalent à α et β ont même caractère de résiduacité k-ique modulo p . Or il y a exactement k tels caractères, donc, par le principe des tiroirs, au moins deux racines ont même caractère, donc $\bar{F}_n = 0$ pour $n = (p - 1)/k$. Toute autre solution inférieure à n divise n .

Par exemple, si pour $p = 11$ et $r = 5$, on a 5 facteurs linéaires, alors $F_{10/5} = F_2 \equiv 0 \mod p$; mais aussi $F_{10/2} = F_5 \equiv 0 \mod p$, ce qui fournit deux familles de zéros de $(\bar{F}_n)$.

10.3. - Pour $p > r$, si (p) a un facteur de norme p^ν , $\nu > 1$, alors pour tout diviseur strict μ de ν $F_{(p^\nu-1)/(p^\mu-1)} \equiv 0 \mod p$.

D'après le théorème de Zolotarev, cela signifie qu'un des facteurs P_i de $\bar{P}(x)$ est de degré ν .

Alors

$$\bar{F}_n(P_i) = 0 \Longleftrightarrow \exists\, \alpha , \alpha' \text{ conjugués } ; \ \eta_n(\alpha) = \eta_n(\alpha')$$
$$\Longleftrightarrow \eta_n \text{ non bijective sur } \{\alpha\}_*$$
$$\Longleftrightarrow \eta_n(\alpha) \in GF(p^\mu) , \ \mu \text{ diviseur strict de } \nu , \text{ par (9.4).}$$

Donc, par (9.5), $n = (p^\nu - 1)/(p^\mu - 1)$ est solution, et toute solution inférieure à n est un diviseur de n .

De part la structure cyclique de $GF(p^\mu)$, il suffit de considérer les μ diviseurs stricts maximaux de ν , sachant que les F_n forment une séquence de divisibilité.

10.4. - Pour $p > r$, si $\bar{P}(x)$ a deux facteurs P_i et P_j de degrés $\nu_i \neq \nu_j$, alors

$$\bar{G}_n(P_i , P_j) = 0 \Longrightarrow \bar{F}_n(P_i) = 0 \text{ ou } \bar{F}_n(P_j) = 0 .$$

Soient $\{\alpha\}_*$ et $\{\beta\}_*$ les ensembles de racines de P_i et P_j .

$$\bar{G}_n(P_i , P_j) = 0 \Longleftrightarrow \exists\, \alpha , \beta \ ; \ \alpha^n = \beta^n .$$

Or, $\alpha^n \in GF(p^{\nu_i})$, et $\beta^n \in GF(p^{\nu_j})$.

Donc

$$\alpha^n = \eta_n(\alpha) \in GF(p^{\nu_i}) \cap GF(p^{\nu_j}) = GF(p^{(\nu_i,\nu_j)}) .$$

Puisque $\nu_i \neq \nu_j$, l'un au moins est différent de (ν_i , ν_j) , donc d'après (9.4), η_n n'est pas bijective sur $\{\alpha\}_*$ ou $\{\beta\}_*$, donc $\bar{F}_n(P_i) = 0$ ou $\bar{F}_n(P_j) = 0$.

10.5. Conclusion.

La condition (ii) du théorème 3 exprime un cas de dégénérescence au cas où $a_r \equiv a_{r-1} \equiv 0 \mod p$. Alors, quel que soit n , $F_n \equiv 0 \mod p$.

Les conditions (i) et (iii) sont résolues par les résultats 10.1 et 10.3.

La condition (iv) est résolue par 10.2 lorsque P_i et P_j sont tous deux du premier degré. La condition (iv) est résolue par 10.4 lorsque P_i et P_j sont de degré différent ; alors aucune famille originale de zéros n'est engendrée par cette condition. Le seul cas non résolu dans la condition (iv) est donc celui où P_i et P_j sont du même degré supérieur à 1.
Mais alors, d'après le résultat 9.6, tout entier i non premier avec $p^\nu - 1$ est solution possible. Pour un tel entier, on peut, en effet, trouver un polynôme $P(x)$ dont la décomposition modulo p fournit deux facteurs P_i et P_j, d'ensembles de racines $\{\alpha\}_*$ et $\{\beta\}_*$, tels que η_i n'est pas bijective sur $\{\alpha\}_* \cup \{\beta\}_*$.

Aucune règle générale n'est donc possible, seule une étude particulière de P_i et P_j permet de décider. Ce cas ne se produit qu'à partir du cas $r = 4$, pour la décomposition $(p) = \mathfrak{p}_2\,\mathfrak{p}_2'$. Ceci nous permet donc de traiter complètement les cas quadratique et cubique. Signalons enfin que notre méthode ne nous permet pas de distinguer les ramifiés $(p|\Delta)$ des pseudo-ramifiés $(p|q_1)$.

Troisième partie : Cas quadratique et cubique.

11. Cas quadratique : $P(x) = x^2 - ax - b$.

La récurrence des F_n est

$$F_{n+2} = aF_{n+1} + bF_n\,,\quad F_0 = 0\,,\quad F_1 = 1\,.$$

Ce sont les nombres de Fibonacci de Lucas.

$p|a$ et $p|b \Longrightarrow \forall\, n > 1\,,\ F_n \equiv 0 \mod p$.

(p) ramifié, $(p) = \mathfrak{p}^2 \Longleftrightarrow p|\Delta = a^2 + 4b \Longrightarrow F_p \equiv 0 \mod p$.

(p) décomposé, $(p) = \mathfrak{p}_1\,\mathfrak{p}_1' \Longleftrightarrow (\Delta/p) = 1 \Longrightarrow F_{p-1} \equiv 0 \mod p\,,\ p > 2$.

(p) inerte, $(p) = \mathfrak{p}_2 \Longleftrightarrow (\Delta/p) = -1 \Longrightarrow F_{p+1} \equiv 0 \mod p\,,\ p > 2$.

12. Cas cubique : $P(x) = x^3 - ax^2 - bx - c$.

La récurrence des F_n est :

$$F_{n+6} = AF_{n+5} + BF_{n+4} + CF_{n+3} + c^2 BF_{n+2} + c^4 AF_{n+1} - c^6 F_n\,,$$

avec

$A = -(ab + 3c)$,
$B = b^3 - 6c^2 - 5abc - a^3 c$,
$C = c(a^2 b^2 + 2b^3 - 7c^2 - 2a^3 c - 6abc)$.
$F_0 = 0$,
$F_1 = 1$,
$F_2 = -(ab + c)$,
$F_3 = b^3 + a^2 b^2 - a^3 c$,
$F_4 = (ab + c)(c^2 - a^2 b^2 + 2a^3 c - 2b^3 + 4abc)$,

$$F_5 = a^6 c^2 - 3a^5 b^2 c - a^4 bc^2 + a^4 b^4 - 8a^3 b^3 c + a^3 c^3 + 3a^2 b^5 - 15a^2 b^2 c^2 + ab^4 c - 8abc^3 - b^3 c^2 + b^6 - c^4 .$$

Ce sont les nombres de Schützenberger d'ordre 3.

$p|b$ et $p|c \Longrightarrow \forall\, n > 1$, $F_n \equiv 0 \mod p$.

$(p) = \mathfrak{p}_1^3 \Longrightarrow F_p \equiv 0 \mod p$,

$(p) = \mathfrak{p}_1^2 \mathfrak{p}_1' \Longrightarrow F_p \equiv 0 \mod p$, et $F_{p-1} \equiv 0 \mod p$,

$(p) = \mathfrak{p}_1 \mathfrak{p}_1' \mathfrak{p}_1'' \Longrightarrow F_{(p-1)/2} \equiv 0 \mod p$,

$(p) = \mathfrak{p}_1 \mathfrak{p}_2 \Longrightarrow F_{p+1} \equiv 0 \mod p$, $p > 3$.

$(p) = \mathfrak{p}_3 \Longrightarrow F_{p^2+p+1} \equiv 0 \mod p$, $p > 3$.

13. Application : $P(x) = x^3 - x - 1$, $\Delta = -23$.

La récurrence des F_n est

$$F_{n+6} = -3F_{n+5} - 5F_{n+4} - 5F_{n+3} - 5F_{n+2} - 3F_{n+1} - F_n .$$

Les premières valeurs, factorisées, des F_n sont les suivantes.

$F_0 = 0$
$F_1 = 1$
$F_2 = -1$
$F_3 = 1$
$F_4 = -1$
$F_5 = -1$
$F_6 = 5$
$F_7 = -2^3$
$F_8 = 7$
$F_9 = 1$
$F_{10} = -19$
$F_{11} = 43$
$F_{12} = -5.11$
$F_{13} = 3^3$
$F_{14} = 2^6$
$F_{15} = -211$
$F_{16} = 7^3$
$F_{17} = -307$
$F_{18} = -5.17$
$F_{19} = 911$
$F_{20} = -19.101$
$F_{21} = 2^3.293$
$F_{22} = -23.43$
$F_{23} = -23.137$
$F_{24} = 5^3.7.11$
$F_{25} = -101.149$
$F_{26} = 3^3.467$
$F_{27} = 53.107$
$F_{28} = 2^7.307$
$F_{29} = 59.1451$
$F_{30} = -5^2.19.211$
$F_{31} = 61.557$
$F_{32} = 7^3.449$
$F_{33} = -43.10\,163$
$F_{34} = 307.2\,143$
$F_{35} = -2^3.64\,189$
$F_{36} = -5.11.17.359$
$F_{37} = 593.3\,329$
$F_{38} = -37.113.911$
$F_{39} = 3^6.5\,851$
$F_{40} = -7.19.79.101$
$F_{41} = -7\,448\,797$

On en déduit que 3 , 13 , 29 , 31 , 41 , non apparus au rang $(p + 1)$ sont inertes.

On voit aussi que 23 a la décomposition $\mathfrak{p}_1^2 \mathfrak{p}_1'$, que 5 , 7 , 11 , 17 , 19 , 37,... ont la décomposition $\mathfrak{p}_1 \mathfrak{p}_2$, et que 53 , 59 , 101 , 149 , 211 , ... ont la décomposition $\mathfrak{p}_1 \mathfrak{p}_1' \mathfrak{p}_1''$.

En ce qui concerne les discriminants, il n'était pas aisé de déterminer que le discriminant de $P_{41}(x)$, polynôme dont les racines sont les puissances 41e de celles de $P(x)$, avait pour discriminant $\Delta_{41} = -(7\,448\,797)^2.23$.

BIBLIOGRAPHIE

[1] BACKSTROM (R. P.). - On the determination of the zeros of the Fibonacci sequence, Fibonacci Quart., t. 4, 1966, p. 313-322.

[2] BERWICK (W. E. H.). - Integral bases. - Cambridge, Cambridge University Press, 1927 (Cambridge Tracts in Mathematics and mathematical Physics, 22).

[3] CARMICHAËL (R. D.). - A simple principle of unification in the elementary theory of numbers, Amer. math. Monthly, t. 36, 1929, p. 132-143.

[4] DELONE (B. N.), FADEEV (D. K.). - The theory of irrationalities of the third degree. - Providence, American mathematical Society, 1964 (translation of mathematical Monographs, 10).

[5] DICKSON (L. E.). - History of the theory of numbers. - New York, Chelsea Publishing Company, 1966.

[6] HORADAM (A. F.). - Basic properties of a certain generalized sequence of numbers, Fibonacci Quart., t. 3, 1965, p. 161-176.

[7] JARDEN (D.). - Recurring sequences. - Jerusalem, Riveon Lematematika, 1958.

[8] LUCAS (E.). - Théorie des nombres. Nouveau tirage. - Paris, A. Blanchard, 1961,

[9] RANEY (G. N.). - Generalization of the Fibonacci sequence to n dimensions, Canad. J. Math., t. 18, 1966, p. 332-349.

[10] WARD (M.). - Prime divisors of second order recurrences, Duke math. J., t. 21, 1954, p. 607-614.

[11] WARD (M.). - Prime divisors of Fibonacci numbers, Pacific J. Math., t. 11, 1961, p. 379-386.

[12] WYLER (O.). - On second order recurrences, Amer. math. Monthly, t. 72, 1965, p. 500-506.

(Texte reçu le 25 février 1978)

Marcel DUBOUÉ
7 rue Courtois
93500 PANTIN