$n(h, r)$ désignant encore ici le plus petit entier n vérifiant les conditions (ii). Les relations (viii), (ix) et (x) nous donnent alors

$$\left|a_n - \sum_{k=0}^{h-1} \varrho^{-kn} A_k(1-\alpha_k) \sin\left(\pi(1-\alpha_k)\right) n^{\alpha_k - 1}/\pi\right| \leqslant K(H, h, r)\, n^{d\langle L\rangle/h-2},$$

ce qui est la relation (4).

References

[1] H. Delange, *Sur la distribution des entiers ayant certaines propriétés*, Ann. Scient. Ec. Norm. Sup., série 3, 73 (1956), p. 15–74.

[2] E. Landau, *Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. (3) 13 (1908), p. 305–312.

[3] G. Rhin, *Répartition modulo* 1 *dans un corps de séries formelles sur un corps fini*, Dissertationes Mathematicae 95, Warszawa 1972.

[4] S. Saks and A. Zygmund, *Analytic functions*, Państwowe Wydawnictwo Naukowe, Warszawa 1959.

[5] J. P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. 22 (3–4) (1976), p. 227–260.

Reçu le 13. 1. 1983
et dans la forme modifiée le 4. 5. 1983 (1335)

ACTA ARITHMETICA
XLIV (1984)

Sur l'irréductibilité des trinômes $X^{p^r+1} - aX - b$ sur les corps finis F_{p^s}

par

S. Agou (Lyon)

Introduction. Soient a, b deux éléments non nuls du corps F_{p^s} et r, $r \geqslant 1$, un entier naturel. On donne dans cet article, lorsque r divise s ou lorsque r est un nombre premier impair une méthode pour déterminer explicitement des conditions d'irréductibilité des trinômes $X^{p^r+1} - aX - b$ sur les corps finis F_{p^s}, généralisant ainsi un travail de Ore [5], sur les polynômes $X^{p^s+1} - \alpha X^{p^s} - \beta X - \gamma$ de $F_{p^s}[X]$.

1. Formules explicites. Les résultats ci-dessous seront utilisés dans la 3ème partie.

1.1. Soient X_1, X_2 deux indéterminées et $F_p(\{X_1, X_2\})$ l'algèbre libre qu'elles engendrent avec F_p.

Pour tout entier naturel n, on désigne par S_n l'ensemble des éléments $\mu = (x_k, y_k, \ldots, x_1, y_1) \in N^{2k}$ où $k = E(n/3)+1$ et où μ est tel que:

1) si pour un indice $i \geqslant 1$ on a $x_i = 0$ alors $x_j = y_j = 0$ pour $j > i$,

2) si pour un indice $i > 1$ on a $y_i = 0$ alors $x_j = y_j = 0$ pour $j \geqslant i$,

3) $\sum_{i=1}^{k} (x_i + 2y_i) = n$.

On désigne par $\sum_n$ la quantité $\sum_{\mu \in S_n} X_1^{x_k} X_2^{y_k} \ldots X_1^{x_1} X_2^{y_1}$ de $F_p(\{X_1, X_2\})$, et on pose $\sum_0 = 1$.

Si $M = X_1^{x_k} X_2^{y_k} \ldots X_1^{x_1} X_2^{y_1}$ est un mot de $F_p(\{X_1, X_2\})$ on appelle poids du mot M, l'entier $\delta(M) = \sum_{i=1}^{k} (x_i + 2y_i)$.

Il est clair que les éléments de S_n correspondent bijectivement aux mots M de $F_p(\{X_1, X_2\})$ tels que $\delta(M) = n$.

Avec ces notations on a la:

1.1.1. Proposition. *Pour tout entier n, $n \geqslant 2$, on a dans $F_p(\{X_1, X_2\})[X]$ l'identité*

$$(1)\quad X^n = \Big(X^{n-2} + \sum_1 X^{n-3} + \ldots + \sum_{n-2}\Big) \cdot (X^2 - X_1 X - X_2) + \sum_{n-1} X + \sum_{n-2} X_2.$$

Preuve. On a $\sum_0 = 1$, $\sum_1 = X_1$.

Pour montrer l'identité (1) il suffit de prouver que $\sum_n = \sum_{n-1} X_1 + \sum_{n-2} X_2$ pour $n \geqslant 2$.

Soit M un mot composant $\sum_n$. Il se termine soit par X_1 soit par X_2. On peut donc écrire $M = M_1 X_1$ ou $M = M_2 X_2$.

On a alors soit $\delta(M) = 1 + \delta(M_1)$ soit $\delta(M) = 2 + \delta(M_2)$.

Ainsi M_1 compose $\sum_{n-1}$ ou M_2 compose $\sum_{n-2}$, et ces éventualités s'excluent mutuellement. Donc M est un mot composant $\sum_{n-1} X_1$ ou $\sum_{n-2} X_2$.

Réciproquement si M_1 est un mot composant $\sum_{n-1}$ et M_2 un mot composant $\sum_{n-2}$ alors $\delta(M_1 X_1) = \delta(M_2 X_2) = n$ et donc $M_1 X_1$ et $M_2 X_2$ sont des mots composant $\sum_n$.

1.2. Dans ce paragraphe, nous allons définir une application $\mathcal{C}$ de $F_p(\{X_1, X_2\})$ dans lui-même généralisant dans une certaine mesure le travail de Ore [5].

Posons $A = F_p(\{X_1, X_2\})$. Soit alors φ un automorphisme de $A[X]$. L'action de φ sur les éléments X_1, X_2, X sera notée exponentiellement, ou de manière habituelle. On définit alors $\mathcal{C}$ de A dans A en posant:

$$\mathcal{C}(X_1) = X_1^{\varphi^{-1}}, \quad \mathcal{C}(X_2) = X_2, \quad \text{avec} \quad \mathcal{C}(M \cdot N) = \varphi^{\delta(N)}(\mathcal{C}(M)) \cdot \mathcal{C}(N),$$

où M et N désignent deux mots de A, où le signe $\cdot$ est mis pour signifier qu'il y a juxtaposition. De plus $\mathcal{C}(1) = 1$.

Enfin si $\lambda \in F_p$, on convient que $\mathcal{C}(\lambda M + N) = \lambda \mathcal{C}(M) + \mathcal{C}(N)$.

Ainsi, par exemple,

$$\mathcal{C}(X_2^{y_1}) = X_2^{(\varphi^{2y_1}-1)/(\varphi^2-1)}; \quad \mathcal{C}(X_1^{x_1}) = X_1^{\varphi^{-1}(\varphi^{x_1}-1)/(\varphi-1)};$$

$$\mathcal{C}(X_1^{x_1} X_2^{y_1}) = X_1^{\varphi^{(2y_1-1)}(\varphi^{x_1}-1)/(\varphi-1))} \cdot X_2^{(\varphi^{2y_1}-1)/(\varphi^2-1)}.$$

On a alors la

1.2.1. Proposition. *Pour tout entier $n \geqslant 2$, l'identité* (1) *de* 1.1 *fournit, à l'aide de la loi $\circ$ de composition des polynômes dans $F_p(\{X_1, X_2\})[X]$, l'identité*

$$(2) \quad X^{\varphi^n} = \Big(\varphi^{n-2} + \varphi^{n-1}\Big(\mathcal{C}\Big(\sum_1\Big)\Big) \cdot \varphi^{n-3} + \ldots + \varphi^2\Big(\mathcal{C}\Big(\sum_{n-2}\Big)\Big)\varphi^0\Big)(X) \circ$$
$$\circ(\varphi^2 - X_1\varphi - X_2\varphi^0)(X) + \varphi\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)X^{\varphi} + \Big(\mathcal{C}\Big(\sum_{n-2} X_2\Big)\Big)X^{\varphi^0}.$$

Preuve. On la démontre en raisonnant par récurrence sur l'entier n.

Pour $n = 2$ on a $X^{\varphi^2} = (\varphi^2 - X_1\varphi - X_2\varphi^0)(X) + X_1 X^{\varphi} + X_2 X^{\varphi^0}$. On déduit aisément de l'hypothèse de récurrence l'égalité:

$$X^{\varphi^{n+1}} = \Big(\varphi^{n-1} + \varphi^n\Big(\mathcal{C}\Big(\sum_1\Big)\Big)\varphi^{n-2} + \ldots + \varphi^3\Big(\mathcal{C}\Big(\sum_{n-2}\Big)\Big)\varphi\Big)(X) \circ$$
$$\circ(\varphi^2 - X_1\varphi - X_2\varphi^0)(X) + \varphi^2\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)X^{\varphi^2} + \varphi\Big(\mathcal{C}\Big(\sum_{n-2}\Big)\Big)X^{\varphi}.$$

Finalement

$$X^{\varphi^{n+1}} = \Big(\varphi^{n-1} + \varphi^n\Big(\mathcal{C}\Big(\sum_1\Big)\Big)\varphi^{n-2} + \ldots + \varphi^3\Big(\mathcal{C}\Big(\sum_{n-2}\Big)\Big)\varphi + \varphi^2\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)\varphi^0\Big)(X) \circ$$
$$\circ(\varphi^2 - X_1\varphi - X_2\varphi^0)(X) +$$
$$+ \varphi\Big(\mathcal{C}\Big(\sum_{n-2} X_2\Big)\Big) + \varphi^2\Big(\mathcal{C}\Big(\sum_{n-1}\Big)X_1\Big)X^{\varphi} + \varphi^2\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)X_2 X.$$

Il reste donc à prouver que:

$$\varphi\Big(\mathcal{C}\Big(\sum_{n-2} X_2\Big)\Big) + \varphi^2\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)X_1 = \varphi\Big(\mathcal{C}\Big(\sum_n\Big)\Big)$$

et

$$\varphi^2\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)X_2 = \mathcal{C}\Big(\sum_{n-1} X_2\Big).$$

La deuxième relation est évidente, quant à la première, elle résulte de la formule $\sum_n = \sum_{n-1} X_1 + \sum_{n-2} X_2$ car

$$\mathcal{C}\Big(\sum_n\Big) = \varphi\Big(\mathcal{C}\Big(\sum_{n-1}\Big)\Big)X_1^{\varphi^{-1}} + \mathcal{C}\Big(\sum_{n-2} X_2\Big).$$

1.2.2. Remarques. (i) Si on substitue à X_1 et X_2 deux éléments x_1 et x_2 du corps F_{p^s}, et si on prend φ tel que $\varphi(x) = x^{p^s}$ pour $x \in F_{p^s}$, alors on retrouve la transformation utilisée par Ore dans [5]. En effet on a $\mathcal{C}(x_1) = x_1$ et $\mathcal{C}(x_2) = x_2$ en prolongeant φ à $A[X]$ en posant $\varphi(X) = X^{p^s}$.

(ii) Soit $F(X) = X^{\varphi^n} + a_{n-1}X^{\varphi^{n-1}} + \ldots + a_0 X^{\varphi^0}$ un polynôme de $F_{p^s}[X]$, avec $\varphi(X) = X^{p^s} = X^{\varphi}$. En exprimant chaque monôme $a_i X^{\varphi^i}$ à l'aide de (2), on met ainsi en évidence deux polynômes $G(X)$ et $R(X)$ tels que:

$$F(X) = G(X) \circ (\varphi^2 - X_1\varphi - X_2\varphi^0)(X) + R(X).$$

On observera que $R(X)$ est le reste de la division euclidienne de $F(X)$ par $X^{\varphi^2} - X_1 X^{\varphi} - X_2 X^{\varphi^0}$ et que $G(X^{\varphi^2} - X_1 X^{\varphi} - X_2 X^{\varphi^0})/(X^{\varphi^2} - X_1 X^{\varphi} - X_2 X^{\varphi^0})$ en est le quotient.

(iii) Il est clair que ce qui précède peut être étendu au cas de l'algèbre libre $F_p(\{X_i\}_i)$ à un nombre fini quelconque d'indéterminées. Nous allons

passer maintenant à l'étude des polynômes $f(X) = X^{p^r+1} - aX - b$ de $F_{p^s}[X]$.

2. Hyponormalité de $X^{p^r+1} - aX - b$.

RAPPELS. Un polynôme f de $F_{p^s}[X]$ est dit *hyponormal* sur F_{p^s} s'il existe une racine x_0 telle que pour toute racine x de f on ait l'inclusion, $F_{p^s}(x_0) \subset F_{p^s}(x)$ (cf. [2]; [3]). L'entier $[F_{p^s}(x_0): F_{p^s}]$ s'appelle le degré minimum de f sur F_{p^s}. On se propose ci-dessous de donner des conditions suffisantes d'hyponormalité de $X^{p^r+1} - aX - b$ sur le corps fini F_{p^s}.

2.1. Si le polynôme $f(X) = X^{p^r+1} - aX - b$ a une racine x_0 dans F_{p^s} alors il est évidemment hyponormal sur F_{p^s}. L'élément $x_0 + 1/x$ de la clôture algébrique $\overline{F_{p^s}}$ de F_{p^s} est une racine de f si et seulement si

$$\left(x_0^{p^r} + \frac{1}{x^{p^r}}\right)\cdot\left(x_0 + \frac{1}{x}\right) - a\left(x_0 + \frac{1}{x}\right) - b = 0,$$

c'est-à-dire si et seulement si x est racine de

$$X^{p^r} + \frac{x_0^2}{b}X + \frac{x_0}{b}.$$

Or on sait que ce dernier polynôme est hyponormal sur F_{p^s} et on a donné dans [1] les degrés des polynômes irréductibles qui le factorisent dans $F_{p^s}[X]$, une fois connue effectivement la racine x_0. Comme il est clair que les polynômes minimaux sur F_{p^s} de x et de $x_0 + 1/x$ ont les mêmes degrés, il en résulte que l'on a une description complète des degrés des irréductibles factorisant $f(X)$.

2.2. Si le polynôme $f(X) = X^{p^r+1} - aX - b$ n'a pas de racine dans F_{p^s} soit alors n_0 le plus petit des degrés des irréductibles qui le factorisent dans $F_{p^s}[X]$. Soit alors f_{n_0} un irréductible de degré n_0 divisant f.

Soit n le degré d'un irréductible f_n, f_n divisant f, avec $n > n_0$ s'il en existe. Dans le cas contraire il est évident que f est hyponormal sur F_{p^s}.

Soient x, x' deux racines distinctes de f_n, x_0, x_0' deux racines distinctes de f_{n_0}.

On a donc

$$x^{p^r} = a + \frac{b}{x}, \quad x_0^{p^r} = a + \frac{b}{x_0}, \quad x_0'^{p^r} = a + \frac{b}{x_0'}.$$

Il en résulte que

$$\frac{x^{p^r} - x_0'^{p^r}}{x^{p^r} - x_0^{p^r}} = \frac{x_0}{x_0'}\cdot\frac{x - x_0'}{x - x_0}.$$

Par récurrence sur l'entier m, on en déduit que

$$\frac{x^{p^{mr}} - x_0'^{p^{mr}}}{x^{p^{mr}} - x_0^{p^{mr}}} = \left(\frac{x_0}{x_0'}\right)^{(p^{mr}-1)/(p^r-1)}\frac{x - x_0'}{x - x_0}.$$

En particulier pour m tel que mr soit le p.p.c.m. $[r, sn]$, de r et de sn, on obtient que

$$\left[1 - \left(\frac{x_0}{x_0'}\right)^{(p^{mr}-1)/(p^r-1)}\right]x^2 - \left[x_0'^{p^{mr}} + x_0 - x_0^{p^{mr}}\left(\frac{x_0}{x_0'}\right)^{(p^{mr}-1)/(p^r-1)} - x_0'\left(\frac{x_0}{x_0'}\right)^{(p^{mr}-1)/(p^r-1)}\right]x + x_0 x_0'^{p^{mr}} - x_0^{p^{mr}} x_0'\left(\frac{x_0}{x_0'}\right)^{(p^{mr}-1)/(p^r-1)} = 0.$$

Puisque $x, x' \notin F_{p^{sn_0}}$ il en résulte ou bien que $F_{p^{sn_0}}(x) = F_{p^{2sn_0}}$ soit $n = 2(n, n_0)$, où (n, n_0) désigne le p.g.c.d. de n et n_0, avec $n_0/(n, n_0)$ impair, ou bien que

$$\left(\frac{x_0}{x_0'}\right)^{(p^{[r,sn]}-1)/(p^r-1)} = 1 \quad \text{et} \quad x_0'^{p^{[r,sn]}} - x_0' = x_0^{p^{[r,sn]}} - x_0$$

$$\text{et} \quad x_0 x_0'^{p^{[r,sn]}} = x_0^{p^{[r,sn]}} x_0'.$$

Ces dernières relations entraînent que $n_0 | rn/(r, sn)$. Finalement en récapitulant les conditions, on a, puisque $n > n_0$,

$$C_1 \begin{cases} n = 2n_0 \\ \text{ou} \\ n_0 | rn/(r, sn). \end{cases}$$

Dans l'étude précédente, il est clair que l'on peut substituer respectivement x_0 à x; x et x' à x_0 et x_0' et m_0 à m où m_0 est tel que $m_0 r = [r, sn_0]$. D'où les conditions:

$$C_2 \begin{cases} n_0 | n, \\ \text{ou} \\ n_0 \nmid n \text{ et } n_0 | 2n, \\ \text{ou} \\ n | rn_0/(r, sn_0). \end{cases}$$

Finalement, C_1 et C_2 fournissent

$$C \begin{cases} n_0 | n, \\ \text{ou} \\ n_0 \nmid n \text{ et } n_0 | 2n \text{ et } n_0 | rn/(r, sn), \\ \text{ou} \\ [r, sn] = [r, sn_0]. \end{cases}$$

On en déduit alors la

2.3. Proposition. *Si l'entier $r/(r, s)$ est primaire(1) impair, alors le polynôme $X^{p^r+1}-aX-b$ est hyponormal sur F_{p^s}.*

Preuve. En effet si $r/(r, s)$ est primaire impair les conditions C se réduisent à $n_0|n$ ou $n=2n_0$.

Comme conséquence immédiate, on en tire la

2.3.1. Proposition. *Si le polynôme $X^{2^r+1}-aX-b$ n'a pas de racine dans F_{2^s}, si $r|s$ et si 2^r+1 est un nombre premier, alors ce polynôme est irréductible sur F_{2^s}.*

Preuve. C'est évident.

Rappelons que les seuls cas connus où 2^r+1 est un nombre premier, pour $r \geqslant 1$, sont lorsque, $2^r+1 \in \{3, 5, 17, 257, 65537\}$.

2.4. Remarque. Si $r/(r, s)$ est primaire impair et si $(r/(r, s), p^r+1)=1$ alors il est loisible de se placer dans $F_{p^{[r,s]}}[X]$ pour étudier le degré minimum de $X^{p^r+1}-aX-b$ sur F_{p^s}. En effet $X^{p^r+1}-aX-b$ reste hyponormal sur $F_{p^{[r,s]}}$ et a même degré minimum sur F_{p^s} et sur $F_{p^{[r,s]}}$.

2.5. Remarque. Supposons $r/(r, s)$ primaire impair; puisque le raisonnement développé dans le paragraphe 2.2 ne s'appuie essentiellement que sur les inégalités $2 \leqslant n_0 < n$, il en résulte que si $(n_i)_{0 \leqslant i \leqslant k}$ est la suite croissante des degrés des irréductibles qui factorisent $X^{p^r+1}-aX-b$ dans $F_{p^s}[X]$ alors on a $n_i|n_{i+1}$ pour $i=0, \ldots, k-1$.

2.6. Remarque. Initialement j'avais obtenu les conditions $r/(r, s)$ primaire impair et sans facteur carré. C'est A. Schinzel, que je remercie, qui m'a signalé que l'on pouvait s'affranchir de la dernière condition.

3. Conditions explicites.

3.1. On se propose ici, pour r divisant s ou pour r premier impair, de donner une condition nécessaire et suffisante explicite pour que le polynôme $f(X)=X^{p^r+1}-aX-b$ soit irréductible sur F_{p^s}.

Il est loisible de faire l'étude à l'aide du polynôme

$$g(X)=X^{p^r+1}-X-b/a^{p^{[r,s]-r}+1}$$

qui se déduit de $f(X)$ en substituant à X, le monôme $a^{p^{[r,s]-r}}X$. Par commodité on écrira

$$g(X)=X^{p^r+1}-X-\beta.$$

Nous allons, pour ce faire, suivre en partie Ore [5] (ou Serret [6]) en extrapolant la démarche.

Si x est une racine de $g(X)$ on a:

$$(*) \qquad x^{p^r}=\frac{x+\beta}{x}.$$

(1) Un entier est dit *primaire* s'il est égal à 1 ou s'il ne possède qu'un unique diviseur premier.

Soient $M_k=\begin{pmatrix}1 & \beta^{p^{kr}}\\ 1 & 0\end{pmatrix}$, pour $k \in \mathbf{N}$, des matrices et r' un entier tel que $r'r=[r, s]$.

Par itération à l'aide de $(*)$ on obtient:

$$(*, *) \qquad x^{p^{[r,s]}}=\frac{\alpha_{r'}x+\beta_{r'}}{\gamma_{r'}x+\delta_{r'}},$$

où les coefficients $\alpha_{r'}$, $\beta_{r'}$, $\gamma_{r'}$, $\delta_{r'}$, de F_{p^s} sont tels que

$$\begin{pmatrix}\alpha_{r'} & \beta_{r'}\\ \gamma_{r'} & \delta_{r'}\end{pmatrix}=M_{r'-1}\ldots M_0.$$

On en déduit que

$$M_0\cdot\begin{pmatrix}\alpha_{r'} & \beta_{r'}\\ \gamma_{r'} & \delta_{r'}\end{pmatrix}=\begin{pmatrix}\alpha_{r'}^{p^r} & \beta_{r'}^{p^r}\\ \gamma_{r'}^{p^r} & \delta_{r'}^{p^r}\end{pmatrix}\cdot M_0,$$

ce qui fournit les relations

$$\begin{aligned}\alpha_{r'}^{p^r}+\beta_{r'}^{p^r}&=\alpha_{r'}+\beta\gamma_{r'},\\ \gamma_{r'}^{p^r}+\delta_{r'}^{p^r}&=\alpha_{r'},\\ \beta\alpha_{r'}^{p^r}&=\beta_{r'}+\beta\delta_{r'},\\ \beta\gamma_{r'}^{p^r}&=\beta_{r'}.\end{aligned}$$

On en déduit que:

$$(*, *, *) \qquad \begin{cases}\alpha_{r'}+\delta_{r'}\in F_{p^r} \quad \text{et} \quad \alpha_{r'}\delta_{r'}-\beta_{r'}\gamma_{r'}=(-\beta)^{(p^{[r,s]}-1)/(p^r-1)},\\ \alpha_{r'}-\delta_{r'}=\beta^{p^r}\gamma_{r'}^{p^{2r}}+\gamma_{r'}^{p^r}-\beta\gamma_{r'}, \quad \alpha_{r'}\delta_{r'}=\beta\gamma_{r'}^{p^r+1}+(-\beta)^{(p^{[r,s]}-1)/(p^r-1)}.\end{cases}$$

Ainsi le paramètre $\gamma_{r'}$ suffit pour exprimer les éléments de $(*, *)$. Ceci étant, avec les notations ci-dessus on a la

3.1.1. Proposition. *Soit r' l'entier tel que $rr'=[r, s]$. Le polynôme $X^{p^r+1}-aX-b$, n'a pas de racine dans $F_{p^{[r,s]}}$ si et seulement si*

$$\text{p.g.c.d.}\ (X^{p^r+1}-X-\beta,\ \gamma_{r'}X^2+(\beta\gamma_{r'}-\gamma_{r'}^{p^r}-\beta^{p^r}\gamma_{r'}^{p^{2r}})X-\beta\gamma_{r'}^{p^r})=1.$$

En particulier si $\gamma_{r'}X^2+(\beta\gamma_{r'}-\gamma_{r'}^{p^r}-\beta^{p^r}\gamma_{r'}^{p^r})X-\beta\gamma_{r'}^{p^r}$ est irréductible sur $F_{p^{[r,s]}}$ alors ce p.g.c.d. *est* 1.

Preuve. Si x est une racine de $g(X)$, la relation $(*, *)$ montre que $x \in F_{p^{[r,s]}}$ si et seulement si $x=\frac{\alpha_{r'}x+\beta_{r'}}{\gamma_{r'}x+\delta_{r'}}$, c'est-à-dire si et seulement si on a

$$x^{p^r+1}-x-\beta=0 \quad \text{et} \quad \gamma_{r'}x^2+(\delta_{r'}-\alpha_{r'})x-\beta_{r'}=0.$$

Observons que si $\beta_{r'}\gamma_{r'}=0$, alors $X^{p^r+1}-aX-b$ a toutes ses racines dans $F_{p^{[r,s]}}$ et réciproquement car $(*, *)$ fournit la relation $x^{p^{[r,s]}}=x$ pour toute

racine x de $X^{p^r+1}-aX-b$. On obtient donc la première partie de la proposition en remplaçant $\delta_{r'}-\alpha_{r'}$ par son expression à l'aide de $\gamma_{r'}$ (cf. (*, *, *)).

Si $\gamma_{r'}X^2+(\delta_{r'}-\alpha_{r'})X-\beta_{r'}$ est irréductible sur $F_{p[r,s]}$ et si

$$\text{p.g.c.d. } (X^{p^r+1}-X-\beta,\ \gamma_{r'}X^2+(\delta_{r'}-\alpha_{r'})X-\beta_{r'}) \neq 1$$

alors il existe x tel que,

$$x=\frac{\alpha_{r'}x+\beta_{r'}}{\gamma_{r'}x+\delta_{r'}}=x^{p^{[r,s]}} \quad \text{avec} \quad x^{p^r+1}-x-\beta=0,$$

ce qui est contraire aux hypothèses.

On déduit de cette proposition la

3.1.2. Proposition. *Soit r un entier divisant s ou premier impair. Soit $p_1^{\mu_1}\dots p_k^{\mu_k}$ la décomposition en facteurs premiers de p^r+1. Soient $(r_i')_{1\leqslant i\leqslant k}$ les entiers tels que $rr_i'=\left[r, s\dfrac{p^r+1}{p_i}\right]$. Il y a équivalence entre*

(i) *$X^{p^r+1}-aX-b$ est irréductible sur F_{p^s}, et*

(ii) p.g.c.d. $(X^{p^r+1}-X-\beta,\ \gamma_{r_j'}X^2+(\beta\gamma_{r_j'}-\gamma_{r_j'}^{p^r}-\beta^{p^r}\gamma_{r_j'}^{p^{2r}})X-\beta\gamma_{r_j'}^{p^r})=1$, $\gamma_{r_i'}\neq 0$ *pour $1\leqslant i\leqslant k$ et $i\neq j$ où j, $1\leqslant j\leqslant k$, est un indice tel que $2[r,s]\mid rr_j'$ lorsque p est impair et un indice arbitraire si $p=2$.*

Avant de démontrer cette proposition, établissons des résultats préliminaires.

(a) La proposition 3.1.1 montre que le polynôme $X^{p^r+1}-aX-b$ n'a pas de racines dans les corps $F_{p^{rr_i'}}$, pour $1\leqslant i\leqslant k$, si et seulement si on a les conditions

(I) p.g.c.d. $(X^{p^r+1}-X-\beta,\ \gamma_{r_i'}X^2+(\delta_{r_i'}-\alpha_{r_i'})X-\beta_{r_i'})=1$ pour $1\leqslant i\leqslant k$.

Soient n_0 le degré minimum de $X^{p^r+1}-aX-b$ sur F_{p^s} et f_{n_0} un polynôme monique irréductible de degré n_0 de $F_{p^s}[X]$ divisant $X^{p^r+1}-aX-b$.

L'hyponormalité de $X^{p^r+1}-aX-b$ sur F_{p^s} montre que $n_0\mid p^r+1$.

(b) Montrons tout d'abord que les conditions (I) équivalent à l'irréductibilité de $X^{p^r+1}-aX-b$ sur F_{p^s}.

Si les conditions (I) sont satisfaites alors $n_0\nmid(rr_i'/s)$ pour $1\leqslant i\leqslant k$, car dans le cas contraire on aurait $F_{p^{sn_0}}\subset F_{p^{rr_i'}}$ pour un indice i convenable, et par suite f_{n_0} et, donc $X^{p^r+1}-aX-b$ auraient des racines dans $F_{p^{rr_i'}}$ ce qui n'est pas.

Ainsi n_0 satisfait aux conditions $n_0\mid p^r+1$ et $n_0\nmid(rr_i'/s)$ pour $1\leqslant i\leqslant k$. Ceci implique que $n_0\nmid(p^r+1)/p_i$ pour $1\leqslant i\leqslant k$ donc que $n_0=p^r+1$.

Je suis redevable à A. Schinzel qui m'a sugéré cette courte preuve.

Réciproquement si $X^{p^r+1}-aX-b$ est irréductible sur F_{p^s} alors $f_{n_0}=X^{p^r+1}-aX-b$.

Si $r\mid s(p^r+1)$ on a $rr_i'=s\dfrac{p^r+1}{p_i}$ pour $1\leqslant i\leqslant k$, et f_{n_0} ne peut avoir de racine dans les corps $F_{p^{rr_i'}}$ pour $1\leqslant i\leqslant k$, puisque ce sont des souscorps propres de $F_{p^{s(p^r+1)}}$.

Si $r\nmid s(p^r+1)$ alors $rr_i'=rs\dfrac{p^r+1}{p_i}$ pour $1\leqslant i\leqslant k$.

Si f_{n_0} avait une racine dans l'un des corps $F_{p^{rr_i'}}$, pour un indice i convenable, alors $p^r+1\mid r\dfrac{p^r+1}{p_i}$ ce qui est absurde.

Les conditions (I) sont donc établies.

(c) Passons maintenant à la démonstration de la proposition 3.1.2.

Supposons $X^{p^r+1}-aX-b$ irréductible sur F_{p^s}, alors les conditions (I) sont satisfaites. Ces conditions (I) entraînent que $\gamma_{r_i'}\neq 0$ pour $1\leqslant i\leqslant k$ (car dans le cas contraire $X^{p^r+1}-aX-b$ aurait toutes ses racines dans $F_{p^{rr_i'}}$ pour un indice i convenable: cf. observation faite dans la preuve de la proposition 3.1.1).

Il en résulte que les conditions (ii) énoncées dans la proposition sont nécessaires.

Montrons que les conditions (ii) sont suffisantes. Supposons les satisfaites. Alors tous les polynômes intervenant dans les conditions (I) sont *non nuls*.

– Si p est impair, le polynôme $X^{p^r+1}-aX-b$ n'a pas de racines dans $F_{p^{rr_j'}}$ et *a fortiori* est premier à $X^{p^{2[r,s]}}-X$ puisque $F_{p^{2[r,s]}}\subset F_{p^{rr_j'}}$. Donc $X^{p^r+1}-aX-b$ est premier à tout polynôme divisant $X^{p^{2s}}-X$ c'est-à-dire est premier à tout polynôme non nul de $F_{p^s}[X]$ de degré au plus égal à 2. Par suite les conditions (I) sont satisfaites et $X^{p^r+1}-aX-b$ est irréductible sur F_{p^s}.

– Si $p=2$, puisque p.g.c.d. $(X^{p^r+1}-X-\beta,\ \gamma_{r_i'}X^2+(\delta_{r_i'}-\alpha_{r_i'})X-\beta_{r_i'})=1$ pour un indice i alors $X^{p^r+1}-aX-b$ n'a pas de racine dans $F_{p^{2[r,s]}}$. En effet s'il en avait une, le degré minimum n_0 de $X^{p^r+1}-aX-b$ sur F_{p^s} diviserait $2r/(r,s)$. Or $n_0\mid 2^r+1$ donc n_0 est impair, ainsi n_0 diviserait $r/(r,s)$.

– Si $r\mid s$ alors $n_0=1$ ce qui est exclu car $X^{p^r+1}-aX-b$ n'a pas de racine dans $F_{p^{rr_i'}}$.

Ainsi $r\nmid s$ et donc r est premier impair. n_0 serait donc égal à r, puisqu'il ne peut être égal à 1, par suite $r\mid 2^r+1$ d'où $r=3$. Donc $n_0=3$. Mais par hypothèse $X^{p^r+1}-aX-b$ n'a pas de racine dans $F_{p^{[3,s(2^3+1)/3]}}=F_{p^{3s}}$, ce qui est contradictoire.

A fortiori $X^{p^r+1}-aX-b$ est premier à $X^{p^{2s}}-X$ et on peut alors reprendre le raisonnement fait dans le cas p impair. ■

3.1.3. Remarque. (i) On peut bien entendu expliciter la condition

$$\text{p.g.c.d.}\left(X^{p^r+1}-X-\beta,\ \gamma_{r'_j}X^2+(\delta_{r'_j}-\alpha_{r'_j})X-\beta_{r'_j}\right)=1.$$

On trouve pour $p\neq 2$, tous calculs faits, la condition compliquée équivalente

$$\beta_{r'_j}^{p^r+1}+2\beta\beta_{r'_j}\gamma_{r'_j}+\beta(\gamma_{r'_j}-\beta_{r'_j})^{p^r}+\beta(\alpha_{r'_j}-\delta_{r'_j})\left(\gamma_{r'_j}^{p^r}-\frac{\beta}{2}\gamma_{r'_j}-\frac{(\gamma_{r'_j}-\beta_{r'_j})^{p^r}}{2}\right)-$$
$$-\frac{\beta_{r'_j}\gamma_{r'_j}}{2}\left[(\alpha_{r'_j}+\delta_{r'_j})^2-4(-\beta)^{(p^{[r,s]}-1)/(p^r-1)}\right]-\beta_{r'_j}\gamma_{r'_j}^{p^r}\neq 0.$$

Pour $p=2$, à l'aide de la proposition 1.1.1 il vient

$$\beta_{r'_j}^{2^r+1}+\beta_{r'_j}\gamma_{r'_j}(\alpha_{r'_j}+\delta_{r'_j})^{2^r}+\beta\sum_{2^r}^{\sim}(\alpha_{r'_j}+\delta_{r'_j})+\beta_{r'_j}\gamma_{r'_j}^{2^r}+$$
$$+\beta\gamma_{r'_j}^{2^r}(\alpha_{r'_j}+\delta_{r'_j})+\beta^2\delta_{r'_j}^{2^r}\neq 0,$$

où $\sum_{2^r}^{\sim}$ est l'expression obtenue en substituant à X_1, $\alpha_{r'}+\delta_{r'}$, et à X_2, $\beta_{r'}$ dans $\sum_{2^r}$.

Enfin il est immédiat de voir que ces expressions, grâce aux formules $(*, *, *)$ du paragraphe 3.1, sont en fait des polynômes en $\gamma_{r'_j}$.

(ii) Le calcul d'un p.g.c.d. et des $k-1$ coefficients $\gamma_{r'_i}$ sont donc nécessaires et suffisants pour tester l'irréductibilité.

(iii) Tous les résultats de ce paragraphe sont encore valables si $r/(r, s)$ est primaire impair.

3.2. On conserve les notations et hypothèses du paragraphe 3.1. Passons au calcul des coefficients $\alpha_{r'}$, $\beta_{r'}$, $\gamma_{r'}$, $\delta_{r'}$ de la formule $(*, *)$. Soit x une racine de $g(X)=X^{p^r+1}-X-\beta$. Ce polynôme n'a que des racines simples. Il existe $\xi\in\bar{F}_p$, $\xi\neq 0$, tel que $x=\xi^{p^r-1}$.

Ainsi $\xi^{p^{2r}-1}-\xi^{p^r-1}-\beta=0$, c'est-à-dire $\xi^{p^{2r}}-\xi^{p^r}-\beta\xi=0$. Si $[r, s]=rr'\geqslant 2r$ alors par récurrence il vient

$$\xi^{p^{[r,s]}}=u_{r'}\xi^{p^r}+v_{r'}\xi \quad \text{où} \quad u_{r'}, v_{r'}\in F_{p^s},$$

d'où $x^{\frac{p^{[r,s]}-1}{p^r-1}}=u_{r'}x+v_{r'}$. Les coefficients $u_{r'}$, $v_{r'}$ ne dépendent pas de la racine x choisie, donc

$$X^{\frac{p^{[r,s]}-1}{p^r-1}}-u_{r'}X-v_{r'}\equiv 0 \bmod(g(X)).$$

De même on a

$$\xi^{p^{r(r'+1)}}=u_{r'+1}\xi^{p^r}+v_{r'+1}\xi \quad \text{avec} \quad u_{r'+1}, v_{r'+1}\in F_{p^s},$$

donc

$$X^{\frac{p^{r(r'+1)}-1}{p^r-1}}-u_{r'+1}X-v_{r'+1}\equiv 0 \bmod(g(X)).$$

Il en résulte d'une part que $u_{r'+1}=(u_{r'}+v_{r'})^{p^r}$ et $v_{r'+1}=\beta u_{r'}^{p^r}$. D'autre part on en déduit que

$$x^{p^{[r,s]}}=\frac{u_{r'+1}x+v_{r'+1}}{u_{r'}x+v_{r'}},$$

et, par ailleurs

$$x^{p^{[r,s]}}=\frac{\alpha_{r'}x+\beta_{r'}}{\gamma_{r'}x+\delta_{r'}}.$$

D'où les relations

$$\mathrm{R}\begin{cases}u_{r'+1}\gamma_{r'}=\alpha_{r'}u_{r'},\\ u_{r'+1}\delta_{r'}+v_{r'+1}\gamma_{r'}=\alpha_{r'}v_{r'}+\beta_{r'}u_{r'},\\ v_{r'+1}\delta_{r'}=\beta_{r'}v_{r'},\end{cases}$$

puisque $p^r+1>2$.

Si $r'=1$ alors $u_{r'}=1$ et $v_{r'}=0$.

De plus pour toute racine x de $g(X)$ on a:

$$0=x^{p^{[r,s]}}-x^{p^{[r,s]}}=\frac{(u_{r'+1}-\alpha_{r'})x+v_{r'+1}-\beta_{r'}}{(u_{r'}-\gamma_{r'})x+v_{r'}-\delta_{r'}}.$$

Il en résulte que $u_{r'+1}=\alpha_{r'}$; $v_{r'+1}=\beta_{r'}$.

En tenant compte des relations R, et de la relation

$$\alpha_{r'}\delta_{r'}-\beta_{r'}\gamma_{r'}=(-\beta)^{\frac{p^{[r,s]}-1}{p^r-1}}\neq 0,$$

il vient

$$u_{r'}=\gamma_{r'} \quad \text{et} \quad v_{r'}=\delta_{r'}.$$

Mais la première partie de cet article, et particulièrement la remarque qui suit la proposition 1.2.1, nous donne le calcul explicite des coefficients $u_{r'+1}$, $v_{r'+1}$, $u_{r'}$ et $v_{r'}$.

En effet on a

$$\gamma_{r'}=u_{r'}=\varphi\left(\bar{C}\left(\sum_{r'-1}\right)\right), \qquad \delta_{r'}=v_{r'}=\bar{C}\left(\sum_{r'-2}X_2\right),$$
$$\alpha_{r'}=u_{r'+1}=\varphi\left(\bar{C}\left(\sum_{r'}\right)\right), \qquad \beta_{r'}=v_{r'+1}=\bar{C}\left(\sum_{r'-1}X_2\right),$$

où chacune des expressions avec $\sim$ représente le résultat de la substitution de 1 à X_1 et de β à X_2 avec $\varphi(x)=x^{p^r}$ pour $x\in F_{p^s}$.

4. Exemples.

4.1. Prenons $s=8$, $r=4$, $r'=2$ et $b\in F_{2^8}$ tel que $b^8=b^5+b^4+b^3+1$. Soit l'automorphisme $\varphi\colon x\mapsto x^{2^4}$ de F_{2^8}. Alors le polynôme $X^{2^4+1}+X+b$ est irréductible sur F_{2^8}. On a

$$\sum_1 = X_1; \quad \sum_2 = \sum_1 \cdot X_1 + \sum_0 \cdot X_2 = X_1^2 + X_2,$$

d'où

$$\gamma_2 = \varphi\big(\tilde{C}\big(\sum_1\big)\big) = 1; \quad \delta_2 = \tilde{C}(X_2) = b;$$

$$\alpha_2 = \varphi\big(\tilde{C}\big(\sum_2\big)\big) = 1+b^{2^4}; \quad \beta_2 = \tilde{C}\big(\sum_1 X_2\big) = b.$$

On recherche alors le p.g.c.d. de $X^2+(b^{2^4}+b+1)X+b$ et de $X^{17}+X+b$. En procédant modulo $X^2+(b^{2^4}+b+1)X+b$ on trouve que

$$X^{16} \equiv X+1.$$

D'où $X^{17} \equiv X^2+X \equiv (b^{2^4}+b)X+b$.

Il en résulte que $\big(X^{17}+X+b,\ X^2+(b^{2^4}+b+1)X+b\big)=1$.

Ainsi $X^{17}+X+b$ est irréductible sur F_{2^8}, en vertu de la proposition 2.3.1.

4.2. Prenons $s=5$, $r=3$ et $b\in F_{2^5}$ tel que $b^5=b^3+1$. Alors le polynôme $X^{2^3+1}+X+b$ est irréductible sur F_{2^5}. On utilise la proposition 2.3.

On se place dans $F_{2^{15}}[X]$. Ainsi $r=3$, $r'=5$, $\varphi\colon F_{2^{15}} \to F_{2^{15}}$ est tel que $x^{\varphi} = \varphi(x) = x^{2^3}$ pour $x\in F_{2^{15}}$.

Les éléments de S_4 sont (0, 0, 0, 2); (0, 0, 2, 1); (0, 1, 2, 0); (1, 1, 1, 0) et (0, 0, 4, 0).

Ceux de S_3 sont (0, 0, 1, 1); (0, 0, 3, 0); (0, 1, 1, 0). On substitue 1 à X_1 et b à X_2.

On a alors

$$\gamma_5 = \varphi\big(\tilde{C}\big(\sum_4\big)\big) = (b^{2^6+1}+b+b^{2^6}+b^{2^3}+1)^{2^3} = b^3+b^2+b+1,$$

$$\delta_5 = \tilde{C}\big(\sum_3 X_2\big) = b^{2^6+1}+b+b^{2^9+1} = b^4+b,$$

$$\alpha_5 = \varphi\big(\tilde{C}\big(\sum_5\big)\big) = \varphi^2\big(\tilde{C}\big(\sum_4\big)\big)+\varphi\big(\tilde{C}\big(\sum_3 X_2\big)\big) = b^4+b+1,$$

$$\beta_5 = \tilde{C}\big(\sum_4 X_2\big) = \varphi^2\big(\tilde{C}\big(\sum_4\big)\big)\cdot b = b^4+b^2+b,$$

d'où

$$\gamma_5 X^2+(\delta_5+\alpha_5)X+\beta_5 = (b^3+b^2+b+1)X^2+X+b^4+b^2+b = h(X).$$

Mais

$$h(X) = (b+1)^3\left[X^2+\frac{X}{(b+1)^3}+\frac{b^4+b^2+b}{(b+1)^3}\right].$$

L'étude du polynôme $h(X)/(b+1)^3$ revient à étudier $\mathrm{Tr}_{F_{2^5}/F_2}(\zeta)$, où

$$\zeta = (b^4+b^2+b)(b+1)^3 = b^3+b^2+1.$$

Le polynôme minimal de b^2 sur F_{2^5} est X^5+X^3+1, le polynôme minimal de b^3 sur F_{2^5} est $X^5+X^3+X^2+X+1$. On a donc $\mathrm{Tr}_{F_{2^5}/F_2}(\zeta)=1$.

Ainsi $h(X)$ est irréductible sur F_{2^5}; il en résulte que X^9+X+b n'a pas de racine dans $F_{2^{15}}$. Comme ce polynôme est hyponormal sur F_{2^5}, il s'ensuit qu'il est irréductible sur F_{2^5}.

Bibliographie

[1] S. Agou, *Factorisation sur un corps fini F_{p^n} des polynômes composés $f(X^{p^r}-aX)$ lorsque $f(X)$ est un polynôme irréductible de $F_{p^n}[X]$*, J. Number Theory 9 (1977), p. 229–239.

[2] — *Sur une classe de polynômes hyponormaux sur un corps fini*, Acta Arith. 39 (1981), p. 105–111.

[3] — *Sur la factorisation des polynômes $f(X^{p^{2r}}-aX^{p^r}-bX)$ sur un corps fini F_{p^n}*, J. Number Theory 12 (1980), p. 447–459.

[4] — *Degré minimum des polynômes $f\big(\sum_{i=0}^{m} a_i X^{p^{r_i}}\big)$ sur les corps finis de caractéristique $p>m$*, Pacific J. Math. 102 (1982), p. 1–8.

[5] O. Ore, *Contributions to the theory of finite fields*, Trans. Amer. Math. Soc. 36 (1934), p. 243–274.

[6] J. A. Serret, *Sur les fonctions rationnelles linéaires prises suivant un module premier...*, C. R. Acad. Sci. Paris 48 (1859), p. 112–117.

UNIVERSITÉ DE LYON 1
Lyon, France

Reçu le 28.1.1983
et dans la forme modifiée le 7.12.1983 (1338)

ACTA ARITHMETICA
XLIV (1984)

On a diophantine equation connected with the Fermat equation.

by

B. Brindza (Debrecen)

1. Introduction. Let $p > 2$ be a prime. In 1946 Inkeri [3] proved that there exists at most a finite number of positive integer triplets (x, y, z) which satisfy the conditions

$$x^p + y^p = z^p, \quad (x, y, z) = 1, \tag{1}$$

and for which at least one of the differences $|x-y|$, $z-x$, $z-y$ is less than a given positive number M. That (1) has only a finite number of solutions x, y and z with $y-x = v$ for v a fixed positive integer, was proved by Everett [2] by means of Roth's famous theorem [7] on approximation of algebraic numbers. Recently Stewart [8] and Inkeri and van der Poorten [5] (in the case where n is a prime) have shown that, for any positive number C_0, all positive integer solutions $x, y, z > 1$, $n > 2$, of the equation

$$x^n + y^n = z^n \quad \text{with} \quad |x-y| < C_0$$

satisfy $\max\{n, x, y, z\} < C$, where C is an effectively computable constant depending only on C_0. Their proofs involve the Gelfond–Baker method.

In [4] Inkeri studied the equation

$$h^p(x) + g^p(x) = z^p. \tag{2}$$

He proved that if h and g are distinct non-constant polynomials with integer coefficients which satisfy the conditions

$$D(g - \zeta^r h) \neq 0 \quad (r = 0, 1, \ldots, p-1); \qquad R(g, h) \neq 0,$$

where $D(\cdot)$ is the discriminant, $R(\cdot, \cdot)$ the resultant and ζ a primitive pth root of unity, then equation (2) has at most a finite number of solutions in rational integers x, z and all these solutions can effectively be determined. His proof depends also on the Gelfond–Baker method.

In [1] we have obtained an effective version of the well-known LeVeque's theorem [6] on the hyperelliptic equation. Our result enables us