Groupe d'étude en théorie analytique des nombres

Yves Hellegouarch

Arithmétique dans $\mathbb{F}_q[t]$. Lois de réciprocité, critères de primalité

Groupe d'étude en théorie analytique des nombres, tome 2 (1985-1986), exp. n° 12, p. 1-10

<http://www.numdam.org/item?id=TAN_1985-1986__2__A7_0>

© Groupe d'étude en théorie analytique des nombres
(Secrétariat mathématique, Paris), 1985-1986, tous droits réservés.

L'accès aux archives de la collection « Groupe d'étude en théorie analytique des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Groupe d'étude en
THÉORIE ANALYTIQUE DES NOMBRES
3e année, 1985/86, n° 12, 10 p.

3 février 1986

ARITHMÉTIQUE DANS $\underset{\sim}{F}_q[t]$.
LOIS DE RÉCIPROCITÉ, CRITÈRES DE PRIMALITÉ

par Yves HELLEGOUARCH (*)

Ce texte reprend sur un point mon exposé du 3 février et y apporte quelques compléments. [Pour un autre point, voir [1].]

L'idée générale consiste à montrer que les méthodes élémentaires de la théorie des nombres [3] se transposent à $\underset{\sim}{F}_q[t]$.

Mais c'est plus ou moins facile, et je dois à John BOXALL l'astuce qui me permet de démontrer simplement la loi de réciprocité.

1. Lois de réciprocité dans $\underset{\sim}{F}_q[t]$.

On considère l'anneau de polynômes $\underset{\sim}{F}_q[t]$ comme analogue à $\underset{\sim}{Z}$, et on écrit que $q = \ell^\theta$ avec ℓ premier et $\theta \geq 1$.

Supposons que $q - 1 = hs$ avec h et $s \in \underset{\sim}{N}$, alors $\underset{\sim}{F}_q[t]$ possède un groupe complet de racines h-ièmes de l'unité que je note μ_h .

On considère les homomorphismes,

$$\varphi_h \begin{cases} \underset{\sim}{F}_q^* \longrightarrow \underset{\sim}{F}_q^* \\ x \longmapsto x^h \end{cases}$$

$$\varphi_s \begin{cases} \underset{\sim}{F}_q^* \longrightarrow \underset{\sim}{F}_q^* \\ x \longmapsto x^s \end{cases}$$

En comptant les éléments des $\operatorname{Ker} \varphi_h$ et $\operatorname{Ker} \varphi_s$, on montre facilement (comme lorsque $h = 2$) que :

LEMME 1. - $\operatorname{Ker} \varphi_h = \operatorname{Im} \varphi_s$ et $\operatorname{Ker} \varphi_s = \operatorname{Im} \varphi_h$.

Soit maintenant un polynôme $P \in \underset{\sim}{F}_q[t]$, on pose $|P| = q^{\deg(P)}$. Remarquons alors que $|P| - 1$ est toujours divisible par $q - 1$, donc par h , donc que $|P| - 1 = hs'$ avec $s' \in \underset{\sim}{N}$.

Définition 1. - On désigne par $\mathcal{M}$ le monoïde multiplicatif des polynômes unitaires de $\underset{\sim}{F}_q[t]$.

(*) Yves HELLEGOUARCH, Département de Mathématiques, Université de Caen, Esplanade de la Paix, 14032 CAEN CEDEX.

Si $P \in \mathbb{M}$, si P est irréductible, et si $Q \in \underset{\sim}{F}_q[t]$, Q non divisible par P, on pose

$$\left(\frac{Q}{P}\right)_h = \varphi_{s'}(Q) \in \mu_h .$$

Ainsi $(Q/P)_h$ désigne la racine h-ième de l'unité dans le corps des constantes $\underset{\sim}{F}_q$ de l'anneau $\underset{\sim}{F}_q[t]$ qui vérifie la condition

$$\left(\frac{Q}{P}\right)_h \equiv Q^{(|P|-1)/h} \quad \text{(modulo } P) .$$

THÉORÈME 1. - Si P et Q sont des polynômes unitaires irréductibles et distincts, on a

$$\left(\frac{P}{Q}\right)_h : \left(\frac{Q}{P}\right)_h = \begin{cases} -1 \text{ si } q \text{ est pair,} \\ (-1)^{((|P|-1)/h)(|Q|-1)/h} \text{ sinon.} \end{cases}$$

Avant de passer à la démonstration de ce théorème, nous énoncerons le lemme suivant.

LEMME 2. - Posons $q^d - 1 = hs'$. Soit N la norme $\underset{\sim}{F}_{q^d}^* \longrightarrow \underset{\sim}{F}_q^*$. Alors on a

$$\varphi_{s'} = \varphi_s \circ N .$$

Preuve. - Si $x \in \underset{\sim}{F}_{q^d}^*$, on a

$$N(x) = x^{1+q+\cdots+q^{d-1}} = x^{(q^d-1)/(q-1)} = x^{s'/s} .$$

D'où

$$\varphi_{s'}(x) = x^{s'} = \varphi^s[N(x)] .$$

Démonstration du théorème 1. - Notations :

$$\begin{cases} |P| = q^d = 1 + ks' \\ |Q| = q^e . \end{cases}$$

1° Dans $\underset{\sim}{F}_{q^d}$ le polynôme P se décompose en facteurs du premier degré

$$P(t) = (t - \alpha_1) \ldots (t - \alpha_d) ,$$

donc les conjugués (non nécessairement distincts) de Q pour l'action du groupe de Galois de $\underset{\sim}{F}_{q^d}/\underset{\sim}{F}_q$ sont

$$Q(\alpha_1) , \ldots , Q(\alpha_d)$$

et

$$\prod_{i=1}^{d} Q(\alpha_i) = N(Q) .$$

D'après le lemme 2, on a donc

$$\varphi_{s'}(Q) = \varphi_s[N(Q)] \equiv R(P , Q)^s \pmod{P}$$

avec

$$R(P , Q) := \prod_{i=1}^{r} Q(\alpha_i) \in \underset{\sim}{F}_q^* .$$

Puisque la réduction modulo P est injective sur $\underset{\sim}{F}_q^*$, on a

$$\left(\frac{Q}{P}\right)_h = R(P , Q)^s .$$

2° Pour la même raison

$$\left(\frac{Q}{P}\right)_h = R(Q , P)^s .$$

3° Il est bien connu que

$$R(P , Q) : R(Q , P) = (-1)^{de} ,$$

d'où

$$R(P , Q) : R(Q , P) = (-1)^{de}$$

et

$$[R(P , Q) : R(Q , P)]^s = (-1)^{sde} ,$$

c'est la loi de réciprocité sous forme générale.

4°(a) Si q est impair, montrons que

$$sde \equiv \frac{|P| - 1}{h} \times \frac{|Q| - 1}{h} \pmod{2} .$$

Nous avons en effet

$$\frac{|P| - 1}{h} = \frac{q^d - 1}{h} = \frac{q - 1}{h} (q^{d-1} + \ldots + 1)$$

$$= s (q^{d-1} + \ldots + 1)$$

$$\equiv sd \pmod{2}$$

de même

$$\frac{|Q| - 1}{h} \equiv se \pmod{2}$$

D'où

$$\frac{|P| - 1}{h} \times \frac{|Q| - 1}{h} \equiv s^2 \text{ de } \equiv \text{sde} \pmod 2 .$$

4°(b) Si q est une puissance de 2, alors s, d et e sont nécessairement impairs.

Remarques importantes. - Dans la suite, nous considérons les applications

$$\begin{cases} \epsilon_h : P \longmapsto \dfrac{|P| - 1}{h} + 2\underset{\sim}{Z} \in \underset{\sim}{Z}/2\underset{\sim}{Z} \\ \theta_h : P \longmapsto \dfrac{|P| - 1}{h} + h\underset{\sim}{Z} \in \underset{\sim}{Z}/h\underset{\sim}{Z} . \end{cases}$$

Un calcul simple donne

$$\frac{|PQ| - 1}{h} = h\left(\frac{|P| - 1}{h}\right)\left(\frac{|Q| - 1}{h}\right) + \frac{|P| - 1}{h} + \frac{|Q| - 1}{h}$$

$$= \frac{|P| - 1}{h} + \frac{|Q| - 1}{h} + hs' t' ,$$

donc θ_h est toujours un morphisme de $\mathfrak{M}$ dans le monoïde additif $\underset{\sim}{Z}/h\underset{\sim}{Z}$.

Si q est impair, $hs' t' \in 2\underset{\sim}{Z}$, donc ϵ_h **est aussi un morphisme de monoïdes.**

2. Symbole de Jacobi.

Soit $N = P_1 \dots P_r \in \mathfrak{M}$, où les P_i sont irréductibles et non nécessairement distincts, et soit $X \in \underset{\sim}{F}_q[t]$.

Définition 2.

$$\begin{cases} \left(\frac{X}{N}\right)_h := \left(\frac{X}{P_1}\right)_h \dots \left(\frac{X}{P_r}\right)_h \quad \text{si} \quad (X , N) = 1 \\ \left(\frac{X}{N}\right)_h := 0 \quad \text{sinon.} \end{cases}$$

THÉORÈME 2.

1° Si $\lambda \in \mu_h$, on a $\left(\frac{\lambda}{N}\right)_h = \lambda^{(|N|-1)/h}$.

2° Si N et $M \in \mathfrak{M}$ et si q est impair, on a

$$\left(\frac{M}{N}\right)_h : \left(\frac{N}{M}\right)_h = (-1)^{\epsilon_h(M)\epsilon_h(N)} .$$

Preuve.

$$1^\circ \qquad \left(\frac{\lambda}{N}\right)_h := \left(\frac{\lambda}{P_1}\right)_h \cdots \left(\frac{\lambda}{P_r}\right)_h$$

$$= \lambda^{\theta_h(P_1)+\cdots+\theta_h(P_r)}$$

$$= \lambda^{\theta_h(P_1 \cdots P_r)} .$$

2° Comme pour le cas quadratique on raisonne par récurrence sur le nombre de facteurs premiers de M et N.

Le problème essentiel revient à montrer que

$$\left(\frac{M}{N_1 N_2}\right) : \left(\frac{N_1 N_2}{M}\right) = (-1)^{\varepsilon_h(M)\varepsilon_h(N_1 N_2)}$$

lorsque l'on suppose que

$$\begin{cases} \left(\frac{M}{N_1}\right) : \left(\frac{N_1}{M}\right) = (-1)^{\varepsilon_h(M)\varepsilon_h(N_1)} , \\ \left(\frac{M}{N_2}\right) : \left(\frac{N_2}{M}\right) = (-1)^{\varepsilon_h(M)\varepsilon_h(N_2)} . \end{cases}$$

Cela résulte de la définition de $(M/N_1 N_2)$, de la multiplicativité de la fonction $x \longmapsto (X/M)$ et du fait que ε_h est un morphisme.

Résumé. - Pour calculer $(X/N)_h$ on peut donc procéder comme dans le cas quadratique, la seule difficulté qui reste à examiner consiste à calculer $(\lambda/N)_h$ lorsque $\lambda \in \underset{\sim}{F}_q^* \setminus \mu_h$ (sans décomposer N en facteurs premiers). Je ne sais pas résoudre cette difficulté dans la cas général, mais on peut toutefois remarquer que cette question admet une réponse évidente lorsque h et s sont premiers entre eux.

COROLLAIRE. - On suppose que $q - 1 = hs$ avec $(h, s) = 1$, alors, si $\lambda \in \underset{\sim}{F}_q^*$, on a

$$\left(\frac{\lambda}{N}\right)_h = \lambda^{(|N|-1)/h} .$$

Preuve.

1° Soit ζ un générateur de $\underset{\sim}{F}_q^*$, comme il existe $\alpha \in \underset{\sim}{N}$ tel que $\lambda = \zeta^\alpha$, il suffit de montrer la formule pour ζ.

2° On sait que $\zeta^s \in \mu_h$, donc (théorème 2)

$$\left(\frac{\zeta^s}{N}\right)_h = \zeta^{s(|N|-1)/h} = (\zeta^{(|N|-1)/h})^s .$$

Mais $(\zeta^s/N)_h = (\zeta/N)_h^s$, d'où l'équation en $x = (\zeta/N)_h$,

$$x^s = (\zeta^{(|N|-1)/h})^s \in \mu_h .$$

Comme s est premier avec h , cette équation possède une solution unique, donc

$$(\frac{\zeta}{N})_h = \zeta^{(|N|-1)/h} .$$

Terminons par un critère permettant de dire si un élément de $\mathfrak{M}$ est une puissance h-ième.

PROPOSITION 1. - Soit $N \in \mathfrak{M}$. Pour que N soit une puissance h-ième il faut et il suffit que, pour tout $X \in \underset{\sim}{F}_q[t]$ tel que $0 < |X| < |N|$, on ait

$$(\frac{X}{N})_h = 1 .$$

Preuve.

1° La condition est évidemment nécessaire.

2° Supposons que

$$N = P_1^{\alpha_1} \dots P_r^{\alpha_s} D^h \; ; \quad 0 < \alpha_1 < h$$

avec $P_1 , \dots , P_r \in \mathfrak{M}$, irréductibles ; nous voulons montrer que $r = 0$. Il est clair que

$$(\frac{X}{N})_h = (\frac{X}{P_1})^{\alpha_1} \dots (\frac{X}{P_r})^{\alpha_r} .$$

Soit $r \geqslant 1$, et soit $|P_1| - 1 = hs'$. On sait qu'il existe $A_r \in (\underset{\sim}{F}_q[t]/P_1)^*$ tel que $\varphi_{s'}(A_1)$ soit une racine primitive h-ième de l'unité.

D'après le théorème chinois, il existe $X \in \underset{\sim}{F}_q[t]$ tel que

$$\begin{cases} X \equiv A_1 \pmod{P_1} \\ X \equiv 1 \pmod{P_i} \quad 2 \leqslant i \leqslant r . \end{cases}$$

On a alors

$$(\frac{X}{N})_h = (\frac{X}{P_1})^{\alpha_1} \dots (\frac{X}{P_r})^{\alpha_r}$$

$$= [\varphi_{s'}(A_1)]^{\alpha_1} \neq 1 .$$

Comme on peut prendre X tel que $0 < |X| < |N|$ on a une contradiction.

3. Applications "théoriques".

Si je qualifie de "théoriques" les applications qui suivent c'est simplement pour signifier que je ne me pose pas le problème de savoir si les algorithmes auxquels elles conduisent sont meilleurs ou moins bons que l'algorithme de Berlekamp qui est l'arme absolue dans ce domaine [3].

Définition 3. - Soit $B \in \mathbb{F}_q[t]$, $B \neq 0$. Un polynôme $N \in \mathcal{M}$ est dit "pseudo-premier en base B" lorsque l'on a :

$$B^{|N|-1} \equiv 1 \pmod{N} .$$

Exemple. - Si $\Phi_n(X)$ désigne le polynôme cyclotomique d'ordre n, et si B est un polynôme non constant, alors $N = \Phi_n(B)$ s'écrit sous la forme

$$N = P_1^{\alpha_1} \dots P_r^{\alpha_r} ,$$

P_i unitaires irréductibles distincts.

Puisque B est une racine primitive n-ième de l'unité modulo P_i, on voit que n divise $|P_i| - 1$ pour tout i.

Il en résulte (remarque du paragraphe 1) que

$$\frac{|N| - 1}{n} \equiv \sum_{i=1}^{r} \alpha_i \frac{|P_i| - 1}{n} \pmod{n}$$

donc

$$B^{|N|-1} \equiv 1 \pmod{N} .$$

Remarque. - On utilise ici le fait que $(\mathbb{F}_q[t]/P_i^{\alpha_i})^*$ est la somme directe de $(\mathbb{F}_q[t]/P_i)^*$ et d'un ℓ-groupe.

On suppose maintenant que $q - 1 = hs$ et que $N \in \mathcal{M}$ est pseudo-premier en base B. On écrit

$$|N| - 1 = h^{\nu} \sigma , \quad 0 < \nu ,$$

avec $(h , \sigma) = 1$, et on pose

$$\begin{cases} B_0 = B^{\sigma} \\ B_1 = B_0^{h} \\ \vdots \\ B_{\nu} = B_{\nu-1}^{h} . \end{cases}$$

Il est clair que $B_{\nu} \equiv 1$ (modulo N).

On appelle "indice de N" le plus petit entier ρ tel que $B_\rho \equiv 1 \pmod N$.

Si $\rho > 0$, on a donc $B_{\rho-1} \not\equiv 1 \pmod N$.

Définition 4. - Soit N pseudo-premier en base B. On dira que N est h-pseudo-premier fort en base B, si, et seulement si,

$$\begin{cases} \text{Soit } \rho = 0 \\ \text{Soit il existe } \zeta \in \mu_h \text{ tel que } B_{\rho-1} \equiv \zeta \pmod N . \end{cases}$$

Exemple 1. - Tout polynôme premier est évidemment h-pseudo-premier fort pour tout B.

Exemple 2. - Il n'est pas sûr que $\Phi_n(B)$ soit h-pseudo-premier fort en base B, car bien que B soit une racine primitive n-ième modulo P_i, il n'est pas certain que cette racine ne dépend pas de l'indice i.

On pourrait dire que $\Phi_n(B)$ est pseudo-premier "fort-mou".

PROPOSITION 2. - On suppose que N est pseudo-premier d'indice $\rho > 0$ en base B. Alors si N n'est pas h-pseudo-premier fort en base B, deux au moins des p. g. c. d. $(N , B_{\rho-1} - \zeta)$ ne sont pas triviaux lorsque ζ parcourt μ_h.

Preuve.

1° Il existe ζ_1 tel que $B_{\rho-1} \equiv \zeta_1 \pmod{P_1}$.

2° Si $B_{\rho-1} \equiv \zeta_1 \pmod{P_i}$ pour tout i, alors le théorème chinois montrerait que $B_{\rho-1} \equiv \zeta_1 \pmod N$, donc N serait h-pseudo-premier fort, ce qui est contraire à l'hypothèse.

Donc il existe $i \neq 1$ tel que $B_{\rho-1} \not\equiv \zeta_1 \pmod{P_i}$.

Soit alors $\zeta_i \in \mu_h$ tel que $B_{\rho-1} \equiv \zeta_i \pmod{P_i}$, il est clair que $\zeta_1 \neq \zeta_i$, donc $(N , B_{\rho-1} - \zeta_1)$ et $(N , B_{\rho-1} - \zeta_i)$ ne sont pas triviaux.

Définition 5. - On suppose q impair et $(h , s) = 1$ (pour pouvoir calculer le symbole de Jacobi par l'algorithme d'Euclide).

On dira que N est h-pseudo-premier eulérien en base B si, et seulement si,

$$B^{(|N|-1)/h} = \left(\frac{B}{N}\right)_h .$$

THÉORÈME 3. - Tout nombre h-pseudo-premier fort en base B est h-pseudo-premier eulérien en base B.

Preuve. - Posons $N = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, alors

$$\left(\frac{B}{N}\right)_h = \left(\frac{B}{P_1}\right)_h^{\alpha_1} \cdots \left(\frac{B}{P_r}\right)_h^{\alpha_r} .$$

1° Cas ou $\rho = 0$. - On a

$$B_0 = B^\sigma \equiv 1 \pmod N$$

d'où

$$B^\sigma \equiv 1 \pmod{P_i}$$

pour tout i .

On en déduit que

$$\left(\frac{B^\sigma}{P_i}\right)_h = \left(\frac{B}{P_i}\right)_h^\sigma = 1 ,$$

et comme $(\sigma , h) = 1$, on a, pour tout i , $(B/P_i)_h = 1$, d'où $(B/N)_h = 1$.

2° Cas général. - Il est clair que la condition

$$B_{\rho-1} \equiv \zeta \pmod N$$

entraîne que, pour tout i ,

$$B_{\rho-1} \equiv \zeta \pmod{P_i} .$$

On en déduit que $|P_i| - 1$ est divisible par h^ρ et on pose

$$|P_i| - 1 = h^\rho r_i , \text{ avec } r_i \in \underset{\sim}{N} .$$

La remarque du paragraphe 1 entraîne que

$$\frac{|N| - 1}{h^\rho} \equiv \sum_{i=1}^r \alpha_i \frac{|P_i| - 1}{h^\rho} \pmod h .$$

Donc $\sigma h^{\nu-\rho} \equiv \sum \alpha_i r_i \pmod h$.

Or

$$\left(\frac{B_0}{P_i}\right)_h \equiv B_0^{(|P_i|-1)/h} \equiv B_0^{h^{\rho-1} r_i} \pmod{P_i} .$$

Donc

$$\left(\frac{B_0}{P_i}\right)_h = \zeta^{r_i}$$

et

$$\left(\frac{B}{N}\right)_h = \prod_{i=1}^r \left(\frac{B}{P_i}\right)_h^{\alpha_i} = \zeta^{(\sum \alpha_i r_i)/\sigma} = \zeta^{h^{\nu-\rho}} ,$$

$$\zeta^{h^{\nu-\rho}} \equiv B_{\rho-1}^{h^{\nu-\rho}} \equiv B^{(|N|-1)/h} \pmod N .$$

RÉFÉRENCES

[1] HELLEGOUARCH (Yves). - Propriétés géométrico-arithmétiques de l'algèbre de Clifford, Université de Caen, 1986 (Prépublication n° 31).

[2] KNUTH (Donald E.). - The art of computer programming, vol. 2 : Seminumerical algorithms. 2nd édition. - Reading, Addison-Wesley publishing Company, 1981 (Addison-Wesley Series in Computer Science and Information Processing).

[3] VALLÉE (B.). - Critères de primalité : présentation des outils de théorie des nombres, Séminaire "Algorithmes et complexité", Caen 1982/83.