ACTA ARITHMETICA
104.2 (2002)

Résidus quadratiques dans $\mathbb{F}_q[T]$

par

Mireille Car (Marseille)

Étant donné un nombre premier impair p, on désigne par $n(p)$ le plus petit entier strictement positif qui ne soit pas carré modulo p et par $r(p)$ le plus petit nombre premier qui soit carré modulo p. En 1927 Vinogradov démontrait que $n(p) = O(p^{1/(2e^{1/2})}(\log p)^2)$ (cf. [14]), ce résultat étant amélioré par Burgess qui en 1957 établissait que $n(p) = O(p^\alpha)$ pour tout réel $\alpha > 1/(4e^{1/2})$ (cf. [2]). Par ailleurs, en 1942, Linnik établissait sous hypothèse de Riemann la majoration $n(p) = O(p^\varepsilon)$ pour tout $\varepsilon > 0$ (cf. [10]). Enfin, en 1952, toujours sous hypothèse de Riemann, Ankeny établissait la majoration $n(p) = O((\log p)^2)$ (cf. [1]). Cette dernière estimation n'est pas loin d'être optimale puisque, d'après Graham et Ringrose, $n(p) = \Omega(\log p \log\log\log p)$ (cf. [5]). Notons aussi qu' en 1950 Nagell démontrait que $r(p) = O(p^{1/2})$ (cf. [12]), cette majoration étant améliorée ultérieurement par Linnik et Vinogradov qui démontraient que $r(p) = O(p^{1/4+\varepsilon})$ (cf. [15]).

Un problème plus général est celui de la détermination, pour tout entier $k \geq 1$, du plus petit entier $b(k)$ ayant la propriété suivante : pour tout entier a premier à k, il existe un entier x premier à k dans l'intervalle $[1, b(k)]$ tel que ax soit carré modulo k. Une forme voisine de ce problème a été étudiée par A. Zaharescu. Utilisant les travaux de Burgess sur les sommes de caractères, A. Zaharescu a démontré (cf. [17]), que pour tout nombre réel $\varepsilon > 0$,

$$H(k) \ll k^{1/4+\varepsilon},$$

la constante impliquée par le symbole $\ll$ dépendant de ε, $H(k)$ désignant le plus petit entier ayant la propriété suivante : pour tout entier a premier à k, il existe un entier x premier à k dans l'intervalle $[-H(k), H(k)]$ tel que ax soit carré modulo k. Cette majoration lui permet dans ce même article d'obtenir des résultats d'approximation diophantienne. Il formule aussi la conjecture

$$\text{(C)} \qquad H(k) \ll k^\varepsilon.$$

2000 *Mathematics Subject Classification*: 11T06, 11T55.

Nous nous proposons d'étudier un problème analogue pour les polynômes à coefficients dans un corps fini de caractéristique impaire. Nous démontrerons un théorème dont un corollaire aura pour conséquence une version polynomiale de la conjecture (C). Soit q une puissance d'un nombre premier impair. Soit $H \in \mathbb{F}_q[T]$ un polynôme non constant. On désigne par $n(H)$ le plus petit entier k pour lequel existe un polynôme unitaire de degré k de $\mathbb{F}_q[T]$ qui ne soit pas un carré modulo H, et on désigne par $r(H)$, resp. $r'(H)$, le plus petit entier k pour lequel existe un polynôme irréductible unitaire de degré k de $\mathbb{F}_q[T]$ qui soit carré, resp. qui ne soit pas carré, modulo H. On désigne par $N(H)$ le plus petit entier k tel que pour tout polynôme $A \in \mathbb{F}_q[T]$, premier à H, il existe $X \in \mathbb{F}_q[T]$, polynôme unitaire de degré k, premier à H, tel que AX soit carré modulo H. Enfin, on désigne par $R(H)$ le plus petit entier k tel que pour tout polynôme $A \in \mathbb{F}_q[T]$, premier à H, il existe $Q \in \mathbb{F}_q[T]$, polynôme irréductible unitaire de degré k, premier à H, tel que AQ soit carré modulo H. De façon évidente, on a

$$n(H) \le N(H) \le R(H), \quad r(H) \le R(H), \quad r'(H) \le R(H), \quad n(H) \le r'(H).$$

Dans ce qui suit, on établit une majoration des nombres $R(H)$ d'où découle une majoration des nombres $N(H)$. On obtient le

THÉORÈME 1. *Pour tout polynôme $H \in \mathbb{F}_q[T]$ non constant, on a*

$$R(H) \le 1 + 2\left[\log_q\left(2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} + 2\right)\right].$$

On en déduit le corollaire suivant.

COROLLAIRE. *Soit H un polynôme de $\mathbb{F}_q[T]$ tel que $\deg H \ge 2$. Alors,*

$$R(H) \le C(q)\,\frac{\deg H}{\log(\deg H)},$$

où

$$C(q) = 2\log 2 \cdot \frac{4q-1}{q-1} + \frac{2q}{\exp(1)(q-1)\log q} + \frac{1}{\exp(1)}\left(1 - \frac{2\log 2}{\log q}\right).$$

De ce fait $R(H)/\deg H$ et, a fortiori, $N(H)/\deg H$ tend vers 0 lorsque $\deg H$ tend vers $+\infty$. Ce corollaire donne la version polynomiale de la conjecture (C).

En modifiant un tout petit peu la démonstration du théorème 1 dans le cas où H est un polynôme irréductible, on obtient le

THÉORÈME 2. (1) *Pour tout polynôme irréductible $P \in \mathbb{F}_q[T]$, on a*

$$R(P) \le 1 + 2\left[\log_q\left(\deg P + \frac{q+1}{q-1} + \frac{2}{\exp(1)\log q}\right)\right].$$

(2) *Il existe un entier* $\delta(q)$ *tel que pour tout polynôme irréductible* $P \in \mathbb{F}_q[T]$ *de degré* $\geq \delta(q)$, *on ait*

$$R(P) \leq 1 + 2\left[\log_q\left(\deg P + \frac{q+1}{q-1}\right)\right].$$

De plus, $\delta(3) = 5$, $\delta(5) = \delta(7) = 4$, $\delta(9) = 3$, *et* $\delta(q) = 2$ *pour tout entier* $q \geq 11$.

(3) *Soit un entier* $d \geq 1$ *tel que* $q > (d-1)^2$. *Alors*, *pour tout polynôme irréductible* P *de degré* d, *on a* $R(P) = 1$.

Lorsque H n'est pas un polynôme irréductible, les nombres $n(H)$, $r(H)$ ou $r'(H)$ sont d'un moindre intérêt. Une démonstration mettant en œuvre les idées développées dans la démonstration du théorème 1 et dans la troisième partie du théorème 2 permet d'obtenir une majoration des nombres $r(H)$ et $r'(H)$ d'où découle une majoration des nombres $n(H)$. Pour éviter d'être répétitifs, nous ne donnerons pas les détails de cette démonstration qui permet de prouver le

THÉORÈME 3. *Pour tout polynôme* $H \in \mathbb{F}_q[T]$ *non constant*, *on a*

$$r(H) \leq 1 + 2\left[\log_q\left(2\deg H + \frac{q+1}{q-1}\right)\right],$$
$$r'(H) \leq 1 + 2\left[\log_q\left(2\deg H + \frac{q+1}{q-1}\right)\right].$$

Notons aussi que 0 est le plus petit entier k pour lequel existe un polynôme unitaire de degré k de $\mathbb{F}_q[T]$ qui soit un carré modulo H.

Dans tous ces énoncés, ainsi que dans ce qui suit, $[y]$ dénote la partie entière d'un nombre réel y.

Dans une dernière partie, en adaptant au cas non archimédien les idées développées dans [17], on appliquera les résultats obtenus à un problème d'approximation diophantienne dans un corps de séries formelles à coefficients dans le corps fini $\mathbb{F}_q$.

I. Préliminaires. On note $\mathbb{M}$ l'ensemble des polynômes unitaires de $\mathbb{F}_q[T]$. On désigne par $\mathbb{I}$, respectivement par $\mathbb{I}_d$, l'ensemble des polynômes irréductibles unitaires de $\mathbb{F}_q[T]$, respectivement l'ensemble des polynômes irréductibles unitaires de degré d de $\mathbb{F}_q[T]$, et par Π_d le nombre d'éléments de l'ensemble $\mathbb{I}_d$. Pour tout entier $k \geq 1$, on désigne par χ_k le caractère quadratique du groupe multiplicatif du corps $\mathbb{F}_{q^k}$. De façon habituelle, on prolonge ce caractère en 0 en posant $\chi_k(0) = 0$. Si $P \in \mathbb{F}_q[T]$ est un polynôme irréductible et si A est un polynôme non divisible par P, le symbole

de Legendre $\left(\frac{A}{P}\right)$ est défini par

$$\left(\frac{A}{P}\right) = \begin{cases} 1 & \text{si } A \text{ est un carré mod } P, \\ -1 & \text{si } A \text{ n'est pas carré mod } P. \end{cases}$$

Le symbole de Jacobi étend le symbole de Legendre à tout couple (A, H) de polynômes premiers entre eux. On pose, pour A et H polynômes premiers entre eux,

$$\left(\frac{A}{H}\right) = \prod_{\substack{P \in \mathbb{I} \\ P|H}} \left(\frac{A}{P}\right)^{v_P(H)},$$

$v_P(H)$ désignant la valuation P-adique du polynôme H. D'autre part, on prolonge aussi ce symbole à tout couple (A, H) de polynômes non premiers entre eux en posant dans ce cas $\left(\frac{A}{H}\right) = 0$.

On désignera par $\omega(H)$ le nombre de facteurs irréductibles unitaires distincts du polynôme H.

PROPOSITION I.1. *On a*

$$q^n = \sum_{d|n} d\Pi_d, \tag{I.1}$$

$$q^n - \frac{q}{q-1}\, q^{n/2} \le n\Pi_n \le q^n. \tag{I.2}$$

Preuve. La relation (I.2) est une conséquence immédiate de la relation (I.1). La relation (I.1) est donnée par le corollaire 3.21 de [9, p. 84].

PROPOSITION I.2. *Pour tout polynôme H de degré ≥ 2, on a*

$$\omega(H) \le \left(\frac{4q-1}{q-1}\right) \frac{\deg H}{\log_q(\deg H)}. \tag{I.3}$$

Preuve. Soit H un polynôme tel que $\deg H \ge 2$. Alors,

$$\omega(H) - \frac{\deg H}{\log_q(\deg H)} \le \sum_{\substack{P \in \mathbb{I} \\ P|H}} \left(1 - \frac{\deg P}{\log_q(\deg H)}\right) \le \sum_{\substack{P \in \mathbb{I} \\ P|H \\ \deg P < \log_q(\deg H)}} 1.$$

Si $\deg H < q$, cette dernière somme est vide, d'où la majoration (I.3). Supposons $\deg H \ge q$. Alors,

$$\omega(H) - \frac{\deg H}{\log_q(\deg H)} \le \sum_{j=1}^{[\log_q(\deg H)]} \Pi_j,$$

d'où, avec (I.2),

$$\omega(H) - \frac{\deg H}{\log_q(\deg H)} \leq \sum_{j=1}^{[\log_q(\deg H)]} \frac{q^j}{j}.$$

Le lemme 7.1 de [4] nous donne alors,

$$\omega(H) - \frac{\deg H}{\log_q(\deg H)} \leq \frac{3q^{1+[\log_q(\deg H)]}}{2(q-1)[\log_q(\deg H)]}.$$

Si $\deg H \geq q^2$,

$$\omega(H) \leq \frac{\deg H}{\log_q(\deg H)} + \frac{3q \deg H}{(q-1)\log_q(\deg H)} = \left(\frac{4q-1}{q-1}\right)\frac{\deg H}{\log_q(\deg H)}.$$

Si $\deg H < q^2$,

$$\frac{\omega(H)\log_q(\deg H)}{\deg H} \leq \log_q(\deg H) < 2 \leq \frac{4q-1}{q-1}.$$

Proposition I.3. *Soient X et Y deux polynômes unitaires de $\mathbb{F}_q[T]$ premiers entre eux. Alors*,

$$\left(\frac{X}{Y}\right)\left(\frac{Y}{X}\right) = (-1)^{(q-1)\deg(X)\deg(Y)/2}. \tag{I.4}$$

Preuve. L'égalité (I.4) est une conséquence des propriétés des symboles locaux, [13, chap. 14]. Une démonstration plus élémentaire est donnée dans [6, chap. 5] pour des couples de polynômes irréductibles unitaires distincts. Le cas général s'en déduit par multiplicativité.

Proposition I.4. *Soit D un polynôme non constant sans facteur carré. Alors*,

$$\Big|\sum_{a\in\mathbb{F}_{q^k}} \chi_k(D(a))\Big| \leq (\deg D - 1)q^{k/2}. \tag{I.5}$$

Preuve. Ce résultat est établi dans [16, Appendice 5]. Par ailleurs, il est démontré dans le cas où $\mathbb{F}_{q^k}$ est le corps premier dans [8, th. 1.4.1.1].

II. Démonstration des théorèmes 1 et 2

Notation II.1. Soient H un polynôme unitaire non constant, A un polynôme premier à H et k un entier strictement positif. On désigne par $\tau(H,k)$ le nombre de facteurs irréductibles unitaires de degré k de H et par $\Pi(H,A,k)$ le nombre de polynômes irréductibles unitaires P de degré k ne divisant pas H et tels que AP soit carré modulo H.

Proposition II.2. *Soient H un polynôme unitaire non constant de $\mathbb{F}_q[T]$ et un entier $k>0$. Pour tout polynôme A premier à H on a*

$$\text{(II.1)}\qquad \left|\Pi(H,A,k)-\frac{q^k}{k}2^{-\omega(H)}\right| \leq \frac{q^{k/2}}{k}\left(\frac{1}{2}\deg H+\frac{1}{q-1}+2^{-\omega(H)}\right)+\frac{1}{2}\tau(H,k).$$

Preuve. Soit K un polynôme unitaire. Soit

$$H=\prod_{\substack{P\in\mathbb{I}\\ P|K}} P. \tag{1}$$

Alors, H est sans facteur carré. Soit Y un polynôme. Alors, Y est premier à K si et seulement s'il est premier à H. Soit Y un polynôme premier à H. D'après le théorème de Hensel et le théorème des restes chinois, Y est carré modulo K si et seulement si il est carré modulo H. Par suite,

$$\Pi(K,A,k)=\Pi(H,A,k).$$

De façon évidente,

$$\tau(H,k)=\tau(K,k),\qquad \omega(H)=\omega(K),\qquad \deg H\leq\deg K.$$

Il suffit donc d'établir la proposition dans le cas où H est sans facteur carré, ce que nous supposerons désormais.

Soit Y un polynôme premier à H. Alors AY est carré modulo H si et seulement si pour tout polynôme irréductible P divisant H, $\left(\frac{AY}{P}\right)=1$. Par suite,

$$\begin{aligned}\Pi(H,A,k)&=\sum_{\substack{Q\in\mathbb{I}_k\\ (Q,H)=1}}2^{-\omega(H)}\prod_{\substack{P\in\mathbb{I}\\ P|H}}\left\{1+\left(\frac{AQ}{P}\right)\right\}\\ &=\sum_{\substack{Q\in\mathbb{I}_k\\ (Q,H)=1}}2^{-\omega(H)}\sum_{\substack{D\in\mathbb{M}\\ D|H}}\left(\frac{AQ}{D}\right),\end{aligned}$$

soit, après inversion de l'ordre des sommations,

$$2^{\omega(H)}\Pi(H,A,k)=(\Pi_k-\tau(H,k))+\sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq1}}\left(\frac{A}{D}\right)\sum_{\substack{Q\in\mathbb{I}_k\\ (Q,H)=1}}\left(\frac{Q}{D}\right). \tag{2}$$

Posons, pour tout diviseur unitaire D de H,

$$\varepsilon_D=(-1)^{k(q-1)\deg(D)/2}. \tag{3}$$

Alors, avec (I.4),

$$2^{\omega(H)}\Pi(H,A,k) = (\Pi_k - \tau(H,k)) + \sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} \varepsilon_D\Big(\frac{A}{D}\Big) \sum_{\substack{Q\in\mathbb{I}_k\\ (Q,H)=1}} \Big(\frac{D}{Q}\Big),$$

d'où

$$2^{\omega(H)}\Pi(H,A,k) = (\Pi_k - \tau(H,k)) + \sigma_k - \theta_k \tag{4}$$

avec

$$\sigma_k = \sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} \varepsilon_D\Big(\frac{A}{D}\Big) \sum_{\substack{Q\in\mathbb{I}_k\\ (Q,D)=1}} \Big(\frac{D}{Q}\Big), \tag{5}$$

$$\theta_k = \sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} \varepsilon_D\Big(\frac{A}{D}\Big) \sum_{\substack{Q\in\mathbb{I}_k\\ (Q,D)=1\\ Q|H}} \Big(\frac{D}{Q}\Big). \tag{6}$$

Si H n'admet pas de facteur irréductible de degré k, on a $\theta_k = 0$. Sinon,

$$|\theta_k| \le \sum_{\substack{Q\in\mathbb{I}_k\\ Q|H}} \sum_{\substack{D\in\mathbb{M}\\ DQ|H\\ D\neq 1}} 1 = \sum_{\substack{Q\in\mathbb{I}_k\\ Q|H}} (2^{\omega(H/Q)} - 1),$$

$$|\theta_k| \le \tau(H,k)(2^{\omega(H)-1} - 1), \tag{7}$$

cette relation restant valable si $\tau(H,k) = 0$.

Notons $\mathbb{E}_d$ l'ensemble des éléments $a \in \mathbb{F}_{q^k}$ qui sont de degré d sur le corps $\mathbb{F}_q$ et posons, pour d divisant k,

$$T(d,D) = \sum_{a\in\mathbb{E}_d} \chi_k(D(a)). \tag{8}$$

Posons aussi

$$S(k,D) = \sum_{a\in\mathbb{F}_{q^k}} \chi_k(D(a)). \tag{9}$$

Tout $a \in \mathbb{E}_d$ est racine d'un polynôme irréductible $Q \in \mathbb{I}_d$ qui a exactement d racines distinctes dans $\mathbb{E}_d$. Par suite,

$$|T(d,D)| \le d\Pi_d. \tag{10}$$

D'autre part, si $Q \in \mathbb{I}_k$, toute racine a de Q appartient au sous-ensemble $\mathbb{E}_k$, et vérifie l'égalité

$$\chi_k(D(a)) = \Big(\frac{D}{Q}\Big),$$

d'où, avec (5) et (8),

$$k\sigma_k = \sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} \varepsilon_D\left(\frac{A}{D}\right)T(k,D),$$

puis, avec (9) et (10),

$$\left|k\sigma_k - \sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} \varepsilon_D\left(\frac{A}{D}\right)S(k,D)\right| \leq (2^{\omega(H)}-1)\sum_{\substack{d|k\\ d\neq k}} d\Pi_d.$$

Avec (I.1), (I.2) et (I.5), il vient

$$\begin{aligned}|k\sigma_k| &\leq \sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} (\deg D-1)q^{k/2} + (2^{\omega(H)}-1)\frac{q}{q-1}q^{k/2}\\ &= q^{k/2}\sum_{\substack{D\in\mathbb{M}\\ D|H\\ D\neq 1}} \deg D + (2^{\omega(H)}-1)\frac{q^{k/2}}{q-1},\end{aligned}$$

soit,

$$|k\sigma_k| \leq q^{k/2}\left(2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} - \frac{1}{q-1}\right). \tag{11}$$

Avec (4), (7), (11) et à nouveau (I.1) et (I.2) on a

$$\begin{aligned}|k2^{\omega(H)}\Pi(H,A,k) - q^k| \leq q^{k/2}&\left(2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} + 1\right)\\ &+ k\tau(H,k)2^{\omega(H)-1}.\end{aligned}$$

Corollaire II.3. *Soit H un polynôme unitaire non constant de $\mathbb{F}_q[T]$. Alors*,

$$R(H) \leq 1 + 2\left[\log_q\left(2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} + 2\right)\right]. \tag{II.2}$$

Preuve. Soit k un entier tel que

$$q^{k/2} > 2^{\omega(H)-1}\deg H + \frac{2^{\omega(H)}}{q-1} + 2. \tag{1}$$

Soit A un polynôme premier à H. La relation (II.1) jointe à la majoration triviale

$$\tau(H,k) \leq \frac{\deg H}{k},$$

nous donne

$$|k2^{\omega(H)}\Pi(H,A,k)-q^k| \le 2^{\omega(H)-1}\deg H+q^{k/2}\left(2^{\omega(H)-1}\deg H+\frac{2^{\omega(H)}}{q-1}+1\right),$$

d'où

$$k2^{\omega(H)}\Pi(H,A,k)q^{-k/2} \ge q^{k/2}-q^{-k/2}2^{\omega(H)-1}\deg H-\left(2^{\omega(H)-1}\deg H+\frac{2^{\omega(H)}}{q-1}+1\right).$$

La condition (1) vérifiée par k est suffisante pour que

$$k2^{\omega(H)}\Pi(H,A,k)>0.$$

Par suite,

$$R(H)\le k, \tag{2}$$

pour tout entier k vérifiant (1).

COROLLAIRE II.4. *Soit H un polynôme de $\mathbb{F}_q[T]$ tel que $\deg H \ge 2$. Alors*,

$$R(H)\le C(q)\,\frac{\deg H}{\log(\deg H)}, \tag{II.3}$$

où

$$C(q)=2\log 2\cdot\frac{4q-1}{q-1}+\frac{2q}{\exp(1)(q-1)\log q}+\frac{1}{\exp(1)}\left(1-\frac{2\log 2}{\log q}\right). \tag{II.4}$$

Preuve. Avec (II.2) et (I.3).

COROLLAIRE II.5. (1) *Soit P un polynôme irréductible de $\mathbb{F}_q[T]$. Alors*,

$$R(P)\le 1+2\left[\log_q\left(\deg P+\frac{q+1}{q-1}+\frac{2}{\exp(1)\log q}\right)\right]. \tag{II.5}$$

(2) *Il existe un entier $\delta(q)$ tel que pour tout polynôme irréductible $P\in\mathbb{F}_q[T]$ de degré $\ge\delta(q)$, on ait*

$$R(P)\le 1+2\left[\log_q\left(\deg P+\frac{q+1}{q-1}\right)\right]. \tag{II.6}$$

De plus, $\delta(3)=5$, $\delta(5)=\delta(7)=4$, $\delta(9)=3$, *et* $\delta(q)=2$ *pour tout entier* $q\ge 11$.

Preuve. Soient P un polynôme irréductible de $\mathbb{F}_q[T]$ et A un polynôme premier à P. Soit un entier $k\ge 1$. On a $\tau(P,k)\le 1$, d'où, avec (II.1),

$$\begin{aligned}2k\Pi(P,A,k)q^{-k/2} &\ge q^{k/2}-\deg P-\frac{q+1}{q-1}-kq^{-k/2}\\ &\ge q^{k/2}-\deg P-\frac{q+1}{q-1}-\frac{2}{\exp(1)\log q}.\end{aligned}$$

On a donc $N(P) \leq k$ pour tout entier k tel que

$$q^{k/2} > \deg P + \frac{q+1}{q-1} + \frac{2}{\exp(1)\log q}.$$

Soit maintenant un entier k appartenant à l'intervalle $[1, \deg P[$. Alors, $\tau(P,k) = 0$, d'où, avec (II.1),

$$k2^{\omega(H)} \Pi(P, A, k) q^{-k/2} \geq q^{k/2} - \deg P - \frac{q+1}{q-1}.$$

On a donc $R(P) \leq k$ pour tout entier k tel que

$$1 \leq k < \deg P \quad \text{et} \quad q^{k/2} > \deg P + \frac{q+1}{q-1}.$$

Ces deux dernières conditions peuvent être réalisées simultanément si

$$q^{\deg P} > q\left(\deg P + \frac{q+1}{q-1}\right)^2. \tag{1}$$

On a donc

$$R(P) \leq 1 + 2\left[\log_q\left(\deg P + \frac{q+1}{q-1}\right)\right]$$

pour tout polynôme irréductible P dont le degré vérifie la condition (1). Si $q \geq 11$, (1) est réalisée dès que $\deg P \geq 2$. Si $q = 9$, (1) est réalisée dès que $\deg P \geq 3$. Si $q = 5$ ou si $q = 7$, (1) est réalisée dès que $\deg P \geq 4$. Enfin, si $q = 3$, (1) est réalisée dès que $\deg P \geq 5$.

La première partie du corollaire II.5 appliquée à un polynôme irréductible P de degré 1 donne $R(P) \leq 3$. En fait, dans ce cas, on peut déterminer $R(P)$.

Proposition II.6. *Soit P un polynôme irréductible de degré* 1. *Alors*, $R(P) = 1$.

Preuve. Supposons que $P = aT + b$ avec $a \in \mathbb{F}_q^*$ et $b \in \mathbb{F}_q$. Le groupe multiplicatif $\mathbb{F}_q^*$ contient des éléments carrés et des éléments non carrés. Soient u un carré de $\mathbb{F}_q^*$ et $v \in \mathbb{F}_q^*$ un élément non carré. Le polynôme $Q_u = T + u + b/a$ est carré modulo P et le polynôme $Q_v = T + v + b/a$ n'est pas carré modulo P.

Soit P un polynôme irréductible de degré 2. La première partie du corollaire II.5 nous donne $R(P) \leq 2$ et la deuxième partie de ce corollaire nous donne $R(P) = 1$ pour $q \geq 11$. On peut se demander quelle est la valeur exacte de $R(P)$ pour les petites valeurs de q. Dans ce qui suit on montre qu'en fait, $R(P) = 1$.

Proposition II.7. *Soit un entier $d \geq 1$ tel que $q > (d-1)^2$. Alors, pour tout polynôme irréductible P de degré d, on a $R(P) = 1$.*

Preuve. Compte tenu de la proposition précédente il suffit de faire la démonstration dans le cas où $d \geq 2$. Soit P un polynôme irréductible de

degré d. Supposons la fonction $Q \mapsto \left(\frac{Q}{P}\right)$ constante sur l'ensemble des polynômes $Q \in \mathbb{I}_1$. D'après la loi de réciprocité quadratique (I.4), la fonction $Q \mapsto \left(\frac{P}{Q}\right)$ est constante sur l'ensemble des polynômes $Q \in \mathbb{I}_1$. Soit $\sigma \in \{+1, -1\}$ la valeur prise par cette fonction. Alors,

$$\sum_{Q \in \mathbb{I}_1} \left(\frac{P}{Q}\right) = \sigma q,$$

ou encore

$$\sum_{a \in \mathbb{F}_q} \chi_1(P(a)) = \sigma q,$$

d'où, avec (I.5), $q \leq (\deg P - 1)q^{1/2}$, c'est-à-dire, $q^{1/2} \leq d - 1$.

Remarques II.8. Soient H un polynôme unitaire non constant, A un polynôme premier à H et k un entier strictement positif. Désignons par $\nu(H, A, k)$ le nombre de polynômes Y de degré k ne divisant pas H et tels que AY soit carré modulo H. Les arguments utilisés dans la démonstration de la proposition II.2 nous donnent

$$2^{\omega(H)}\nu(H, A, k) = \sum_{\substack{Y \in \mathbb{M} \\ \deg Y = k \\ (Q,H)=1}} 1 + \sum_{\substack{D \in \mathbb{M} \\ D|H \\ D \neq 1}} \left(\frac{A}{D}\right) \sum_{\substack{Y \in \mathbb{M} \\ \deg Y = k \\ (Q,H)=1}} \left(\frac{Y}{D}\right).$$

Pour majorer la dernière somme de caractères on peut établir un analogue polynomial au théorème de Burgess (cf. [3]), d'où l'on peut déduire la majoration $N(H) \ll |H|^{1/4+\varepsilon}$, la constante impliquée par le symbole $\ll$ ne dépendant que de q et de ε.

Cette majoration est nettement moins bonne que la majoration de $R(H)$ obtenue ci-dessus. L'auteur n'a pas réussi a obtenir directement une majoration de $N(H)$ aussi bonne que celle obtenue à partir de la majoration de $R(H)$.

III. Un problème d'approximation diophantienne. Posons $\mathbb{A} = \mathbb{F}_q[T]$, $\mathbb{K} = \mathbb{F}_q(T)$ et notons $\mathbb{K}_\infty$ le complété de $\mathbb{K}$ pour la valuation à l'infini ν définie sur $\mathbb{K}$ par $\nu(0) = +\infty$, $\nu(G/H) = \deg H - \deg G$ si G et H sont des éléments non nuls de $\mathbb{A}$. Notons encore ν l'unique prolongement de la valuation ν au complété $\mathbb{K}_\infty$. Le corps $\mathbb{K}_\infty$ s'identifie au corps $\mathbb{F}_q((T^{-1}))$ des séries de Laurent en T^{-1}. On désigne par $\wp$ l'idéal de valuation de $\mathbb{K}_\infty$. Tout $x \in \mathbb{K}_\infty$ s'écrit de façon unique comme somme

$$x = [x] + \{x\}, \quad [x] \in \mathbb{A}, \ \{x\} \in \wp, \tag{III.1}$$

où $[x]$ est la partie polynomiale de x et $\{x\}$ la partie fractionnaire de x. (On a déjà utilisé et on utilisera encore dans ce paragraphe la notation $[y]$ pour

désigner la partie entière d'un nombre réel y, mais il y a peu de risque de confusion.)

Tout élément $x \in \mathbb{K}_\infty$ peut être approché par des fractions rationnelles. On appelle *fraction de Farey* à l'ordre k toute fraction rationnelle G/H telle que $\deg H \leq k$, $\deg G < \deg H$, $\operatorname{pgcd}(H, G) = 1$. On désigne par $\mathcal{F}_k$ l'ensemble des fractions de Farey à l'ordre k. Si $G/H \in \mathcal{F}_k$, on appelle *arc de Farey* de centre G/H l'ensemble

$$\mathcal{U}_{G/H} = \{x \in \wp \mid \nu(t - G/H) > k + \deg H\}. \tag{III.2}$$

Proposition III.1. *Lorsque G/H décrit l'ensemble des fractions de Farey à l'ordre k, les arcs de Farey $\mathcal{U}_{G/H}$ forment une partition de $\wp$.*

Preuve. C'est le théorème 4.3 de [7].

Nous pouvons maintenant prouver un analogue polynomial au lemme 3 de [17].

Proposition III.2. *Soient H_1 et H_2 des polynômes premiers entre eux. Pour tout entier $k \geq 0$, il existe un polynôme Y et des polynômes X_1 et X_2 tels que*

$$Y^2 = X_1 H_1 + X_2 H_2, \tag{i}$$

$$\deg Y \leq k, \tag{ii}$$

$$\deg X_1 \leq \max(2k - \deg H_1, N(H_1) + \deg H_1 + \deg H_2 - 2k - 2), \tag{iii}$$

$$\deg X_2 \leq N(H_1) + 2\deg H_1 - 2k - 2. \tag{iv}$$

Preuve. D'après la définition du nombre $N(H_1)$, il existe un polynôme Q premier à H_1, de degré $N(H_1)$ tel que QH_2 soit un carré modulo H_1. Soit alors U un polynôme tel que

$$QH_2 \equiv U^2 \bmod H_1. \tag{1}$$

Le polynôme U est inversible modulo H_1. Soit V l'unique polynôme tel que

$$UV \equiv 1 \bmod H_1, \quad \deg V < \deg H_1. \tag{2}$$

D'après la proposition précédente, il existe une fraction de Farey G/Y à l'ordre k telle que V/H_1 appartienne à l'arc de Farey $\mathcal{U}_{G/Y}$. On a donc

$$\nu\left(\frac{V}{H_1} - \frac{G}{Y}\right) > \deg Y + k,$$

d'où

$$\nu\left(\left\{\frac{VY}{H_1}\right\}\right) > k. \tag{3}$$

Soit R l'unique polynôme tel que

$$VY \equiv R \bmod H_1, \quad \deg R < \deg H_1. \tag{4}$$

D'après (3),

$$\deg R < \deg H_1 - k. \tag{5}$$

Avec (1), (2) et (4), on a

$$Y^2 \equiv QH_2R^2 \bmod H_1.$$

Posons

$$X_2 = QR^2. \tag{6}$$

Alors, il existe un polynôme X_1 tel que

$$Y^2 = X_2H_2 + X_1H_1. \tag{7}$$

La majoration (iv) se déduit de (5) et (6). Si $2\deg Y > \deg(X_2H_2)$, on a $\deg(X_1H_1) = 2\deg Y \le 2k$, d'où la majoration (iii). Si $2\deg Y \le \deg(X_2H_2)$, on a $\deg(X_1H_1) \le \deg(X_2H_2) \le N(H_1) + 2\deg H_1 + \deg H_2 - 2k - 2$, d'où la majoration (iii).

Corollaire III.3. *Soient H_1 et H_2 des polynômes premiers entre eux et tels que $\deg H_1 \le \deg H_2$. Pour tout entier $n \ge 0$, il existe un polynôme Y et des polynômes X_1 et X_2 tels que*

(i) $$Y^2 = X_1H_1 + X_2H_2,$$

(ii) $$\deg Y \le n,$$

(iii) $$\deg X_i \le \max\left(\frac{N(H_1)}{2} + \frac{\deg H_2}{2}, N(H_1) + \deg H_1 + \deg H_2 - 2n\right), \quad i = 1, 2.$$

Preuve. La proposition précédente où l'on prend

$$k = \left[\frac{N(H_1)}{4} + \frac{\deg H_1}{2} + \frac{\deg H_2}{4}\right]$$

nous donne l'existence de polynômes Y, X_1 et X_2 vérifiant (i) et tels que

$$\deg Y \le k,$$
$$\deg X_i \le \min\left(\frac{N(H_1)}{2} + \frac{\deg H_2}{2}, N(H_1) + \deg H_1 + \deg H_2 - 2k\right).$$

Soit un entier $n \ge 0$. Si $n \ge k$, les polynômes Y, X_1, X_2 ci-dessus répondent aux conditions du corollaire. Si $n < k$, la proposition III.2 donne l'existence de polynômes Y, X_1 et X_2 répondant aux conditions du corollaire.

Les propositions suivantes nécessitent quelques rappels concernant les *développements en fractions continuées* dans le corps $\mathbb{K}_\infty$. Nous nous référons ici au chapitre 4 de [11]. Tout élément $x \in \mathbb{K}_\infty$ admet un développement fini ou infini en fraction continuée, le développement étant fini si et seulement si $x \in \mathbb{K}$. Ce développement est donné par la suite finie ou infinie (A_n)

d'éléments de $\mathbb{A}$ et la suite finie ou infinie (x_n) d'éléments de $\mathbb{K}_\infty$ déterminées par la condition initiale

$$x_0 = x, \quad A_0 = [x],$$

et la relation de récurrence :

$$\text{si } x_n \neq A_n, \quad x_{n+1} = \frac{1}{x_n - A_n}, \quad A_{n+1} = [x_{n+1}],$$

le procédé s'arrêtant si $x_n = A_n$. La suite des *réduites* de x est la suite des fractions rationnelles (P_n/Q_n) où P_n et Q_n sont les polynômes déterminés par les conditions initiales :

$$P_0 = A_0, \quad Q_0 = 1, \quad P_1 = 1 + A_0A_1, \quad Q_1 = A_1,$$

et les relations de récurrence :

$$P_{n+1} = A_{n+1}P_n + P_{n-1}, \quad Q_{n+1} = A_{n+1}Q_n + Q_{n-1},$$

si celles-ci ont un sens. Pour tout n, les polynômes P_n et Q_n sont premiers entre eux. Les suites $(\deg P_n)$ et $(\deg Q_n)$ sont strictement croissantes. De plus

$$\nu\left(\frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n}\right) = \deg Q_{n+1} + \deg Q_n, \tag{III.3}$$

$$\nu\left(x - \frac{P_n}{Q_n}\right) = \deg Q_{n+1} + \deg Q_n. \tag{III.4}$$

Proposition III.4. *Soit $\alpha \in \mathbb{K}_\infty$. Soient G_1/H_1 et G_2/H_2 deux réduites successives du développement en fraction continuée de α. Alors, il existe un polynôme Y de degré*

$$k = \left[\frac{N(H_1)}{4} + \frac{\deg H_1}{2} + \frac{\deg H_2}{4}\right]$$

tel que

$$\nu(\{Y^2\alpha\}) \geq \tfrac{1}{2}\deg H_2 - \tfrac{1}{2}N(H_1).$$

Preuve. Avec (III.3) et (III.4), on a

$$\nu(\{H_1\alpha\}) = \deg H_2, \quad \nu(\{H_2\alpha\}) > \deg H_2. \tag{1}$$

Soit

$$k = \left[\tfrac{1}{4}(2\deg H_1 + \deg H_2 + N(H_1))\right]. \tag{2}$$

D'après la proposition précédente, il existe un polynôme Y et des polynômes X_1 et X_2 tels que

$$Y^2 = X_1H_1 + X_2H_2, \tag{3}$$

$$\deg Y \leq k, \tag{4}$$

$$\deg X_1 \leq \tfrac{1}{2}\deg H_2 + \tfrac{1}{2}N(H_1), \quad \deg X_2 \leq \tfrac{1}{2}\deg H_2 + \tfrac{1}{2}N(H_1). \tag{5}$$

D'après (1) et (5), pour $i = 1, 2$,

$$\nu(\{H_i\alpha\}X_i) \geq \tfrac{1}{2}\deg H_2 - \tfrac{1}{2}N(H_1),$$

d'où

$$\nu(\{X_iH_i\alpha\}) = \nu(\{\{H_i\alpha\}X_i\}) \geq \tfrac{1}{2}\deg H_2 - \tfrac{1}{2}N(H_1).$$

Avec (3), il vient $\nu(\{Y^2\alpha\}) \geq \frac{1}{2}\deg H_2 - \frac{1}{2}N(H_1)$.

COROLLAIRE III.5. *Soit α un élément non rationnel de $\mathbb{K}_\infty$. Alors, pour tout entier $N > 0$ il existe un polynôme non nul Y tel que* $\deg Y < N$ *et tel que*

$$\nu(\{Y^2\alpha\}) \geq \frac{2N}{3} - C(q)\,\frac{4N/3}{\log(4N/3)}, \tag{III.5}$$

$C(q)$ étant la constante définie par la relation (II.4).

Preuve. Si

$$\frac{2N}{3} - C(q)\,\frac{4N/3}{\log(4N/3)} \leq 0,$$

l'inégalité (III.5) est trivialement vérifiée pour tout polynôme Y. Nous supposerons

$$\frac{2N}{3} - C(q)\,\frac{4N/3}{\log(4N/3)} > 0, \tag{1}$$

ce qui implique, compte tenu de (II.4) que

$$4C(q)N \geq 3\log(4N/3). \tag{2}$$

Soit

$$m = [(4N-3)/3]. \tag{3}$$

Soient G_1/H_1 et G_2/H_2 les deux réduites successives du développement en fraction continuée de α telles que H_2 est le premier dénominateur de degré $\geq m$. On a donc

$$\deg H_1 < m \leq \deg H_2. \tag{4}$$

D'après le corollaire III.3, il existe des polynômes Y, X_1 et X_2 tels que

$$Y^2 = X_1H_1 + X_2H_2, \tag{i}$$

$$\deg Y \leq N - 1, \tag{ii}$$

$$\deg X_i \leq \max\left(\frac{N(H_1)}{2} + \frac{\deg H_2}{2}, N(H_1) + \deg H_1 + \deg H_2 - 2N + 2\right). \tag{iii}$$

On en déduit que

$$\nu(\{H_i\alpha\}X_i) \geq \min\big(\tfrac{1}{2}\deg H_2 - \tfrac{1}{2}N(H_1), 2N - 2 - N(H_1) - \deg H_1\big),$$

d'où

$$\nu(\{Y^2\alpha\}) \geq \min\big(\tfrac{1}{2}\deg H_2 - \tfrac{1}{2}N(H_1), 2N - 2 - N(H_1) - \deg H_1\big).$$

Supposons $\deg H_1 \geq 2$. Alors, d'après le corollaire II.4,

$$\nu(\{Y^2\alpha\})$$
$$\geq \min\left(\frac{1}{2}\deg H_2 - \frac{1}{2}C(q)\,\frac{\deg H_1}{\log(\deg H_1)}, 2N-2-C(q)\,\frac{\deg H_1}{\log(\deg H_1)} - \deg H_1\right),$$

d'où, avec (4),

$$\nu(\{Y^2\alpha\}) \geq \min\left(\frac{m}{2} + \frac{1}{2} - \frac{1}{2}C(q)\,\frac{m}{\log m}, 2N - 1 - C(q)\,\frac{m}{\log m} - m\right). \tag{5}$$

Si $\deg H_1 = 1$, d'après la proposition II.5, $N(H_1) = 1$, d'où,

$$\nu(\{Y^2\alpha\}) \geq \min((m-1)/2, 2N - 2 - m),$$

et, compte tenu de (II.4), la relation (5) est encore vraie. Les relations (3) et (2) donnent alors

$$\nu(\{Y^2\alpha\}) \geq \frac{2N}{3} - C(q)\,\frac{(4N-3)/3}{\log((4N-3)/3)},$$

d'où l'on déduit la relation (III.5).

Corollaire III.6. *Soit $\alpha \in \mathbb{K}_\infty$. Alors, pour tout réel $\varepsilon > 0$, il existe une infinité de polynômes Y tels que*

$$\nu(\{Y^2\alpha\}) \geq (2/3 - \varepsilon)\deg Y.$$

Preuve. Si $\varepsilon \geq 2/3$, l'énoncé est trivial. On suppose $0 < \varepsilon < 2/3$. Si $\alpha \in \mathbb{K}$, il existe des polynômes G et H tels que $\alpha = G/H$ et, pour tout polynôme Z, $\{(HZ)^2\alpha\} = 0$, d'où,

$$\nu(\{(HZ)^2\alpha\}) = \infty > (2/3 - \varepsilon)\deg(HZ).$$

On suppose que $\alpha \notin \mathbb{K}$. Soit N_ε un entier tel que

$$N_\varepsilon \geq \frac{3}{4}\exp\left(\frac{4C(q)}{3\varepsilon}\right). \tag{1}$$

D'après le corollaire III.5, pour tout entier $N \geq N_\varepsilon$, il existe un polynôme Y_N tel que

$$\deg Y_N < N, \tag{2}$$
$$\nu(\{Y_N^2\alpha\}) \geq \frac{2N}{3} - C(q)\,\frac{4N/3}{\log(4N/3)},$$

d'où, avec (1),

$$\nu(\{Y_N^2\alpha\}) \geq (2/3 - \varepsilon)N, \tag{3}$$

puis avec (2),

$$\nu(\{Y_N^2\alpha\}) \geq (2/3 - \varepsilon)\deg Y_N. \tag{4}$$

Comme $\alpha \notin \mathbb{K}$, l'ensemble des polynômes Y_N vérifiant (3) est infini.

Remerciements. L'auteur remercie le rapporteur ainsi que le Professeur Schinzel pour leurs indications et commentaires.

Références

[1] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) 55 (1952), 65–72.
[2] D. A. Burgess, *The distribution of quadratic residues and non residues*, Mathematika 4 (1957), 106–112.
[3] —, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), 179–192.
[4] G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field*, Oxford Math. Monographs, 1991.
[5] S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic non residues*, in: Analytic Number Theory (Allerton Park), Progr. Math. 85, Birkhäuser, 1989, 269–309.
[6] H. Hasse, *Number Theory*, 3rd ed., Grundlehren Math. Wiss. 229, Springer, 1980, Part I, Chap. 5, 100–103.
[7] D. R. Hayes, *The expression of a polynomial as the sum of three irreducibles*, Acta Arith. 11 (1966), 461–488.
[8] N. Katz, *Sommes exponentielles*, Astérisque 79 (1980).
[9] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, 1997.
[10] Yu. V. Linnik, *A remark on the least quadratic non residue*, Dokl. Akad. Nauk SSSR (N.S.) 36 (1942), 119–120.
[11] B. de Mathan, *Approximations diophantiennes dans un corps local*, Bull. Soc. Math. France Mém. 21 (1970).
[12] T. Nagell, *Sur les restes et non restes quadratiques suivant un module premier*, Ark. Mat. 1 (1950), 185–193.
[13] J.-P. Serre, *Corps locaux*, 2ième éd., Actualités Sci. Indust. 1296, Hermann, 1968.
[14] I. M. Vinogradov, *On the bound of the least non-residue of nth powers*, Trans. Amer. Math. Soc. 28 (1927), 218–226.
[15] I. M. Vinogradov and Yu. V. Linnik, *Hyperelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR 168 (1966), 259–261 (in Russian).
[16] A. Weil, *Basic Number Theory*, 3rd ed., Grundlehren Math. Wiss. 144, Springer, 1974.
[17] A. Zaharescu, *Small values of* $n^2\alpha$ (*mod* 1), Invent. Math. 121 (1995), 379–388.

Laboratoire de Mathématiques
Bâtiment Henri Poincaré
Faculté des Sciences de St. Jérôme
Av. Escadrille Normandie Niemen
13397 Marseille Cedex 20, France
E-mail: mireille.car@math.u-3mrs.fr

Reçu le 21.3.2001
et révisé le 6.11.2001 (3998)