ACTA ARITHMETICA
LXIX.1 (1995)

Sur un problème de L. Carlitz

par

Saïd El Baghdadi (Beni-Mellal)

1. Introduction. Dickson a conjecturé en 1909 dans [4] que toute forme binaire $Q(X,Y)$ de degré pair $2r$, $r>1$, à coefficients dans un corps fini $\mathbb{F}_q$ de caractéristique différente de 2 telle que, pour tout (a,b) de $\mathbb{F}_q\times\mathbb{F}_q$ distinct de $(0,0)$, $Q(a,b)$ soit un carré non nul de $\mathbb{F}_q$ est un carré dès que q dépasse une certaine borne N_r qui ne dépend que de r. Cette conjecture a été démontrée en 1947 par Carlitz dans [1] où il a montré que, si d est un entier ≥ 2, q une puissance d'un nombre premier impair telle que $q>(d-1)^2$ et f un élément de $\mathbb{F}_q[X]$ de degré d tel que, pour tout x de $\mathbb{F}_q$, $f(x)$ soit un carré non nul de $\mathbb{F}_q$, f est un carré de $\mathbb{F}_q[X]$. Carlitz est revenu sur cette question dans deux autres articles [2] et [3] démontrant notamment dans [2] que, pour tout entier $d\geq 2$, il existe un entier $N(d)$ tel que, si $q\geq 3$ est une puissance d'un nombre premier impair telle que $q>N(d)$ et si f est un élément de degré d de $\mathbb{F}_q[X]$ tel que, pour tout x de $\mathbb{F}_q$, $f(x)$ soit un carré de $\mathbb{F}_q$, f est un carré de $\mathbb{F}_q[X]$.

Nous reprenons ici ce problème de Carlitz en montrant que, pour d impair, on peut prendre $N(d)=d^2$, que pour d pair ≥ 4, on peut prendre $N(d)=(d-1)^2$ et que ces valeurs de $N(d)$ ne peuvent en général être améliorées; nous montrons aussi, en adaptant une méthode introduite par Stark [9], que lorsqu'on se restreint aux corps finis premiers, on peut prendre $N(d)=(d^2+2d-1)/2$ pour d impair et $(d^2+d-4)/2$ pour d pair et ≥ 4. Nous avons étudié ce problème dans un cadre un peu plus général en définissant des fonctions généralisant la borne $N(d)$ de Carlitz et c'est l'étude de ces dernières qui est à la base de nos résultats.

Je remercie G. Terjanian qui m'a aidé dans ce travail et le rapporteur pour ses remarques qui m'ont permis d'améliorer la rédaction de cet article.

2. Les corps finis premiers. Soient $d\geq 2$ et r deux entiers tels que $0\leq r\leq d$. Dans la suite, on notera $P_{d,r}$ (resp. $Q_{d,r}$ pour d pair) l'ensemble des entiers $q\geq 3$, puissances d'un nombre premier impair tel qu'il existe f (resp. f dont le coefficient dominant est un carré de $\mathbb{F}_q$) dans $\mathbb{F}_q[X]$, non

carré, de degré d, ayant exactement r zéros dans $\mathbb{F}_q$ tel que pour tout élément x de $\mathbb{F}_q$, $f(x)$ soit un carré de $\mathbb{F}_q$. Remarquons que si d est pair, $Q_{d,r} \subset P_{d,r}$.

Notons Π l'ensemble des nombres premiers et introduisons la définition suivante que nous justifierons ci-dessous.

Définition. Soient $d \geq 2$ et r deux entiers tels que $0 \leq r \leq d$. Nous noterons $\lambda_r(d)$ (resp. $\mu_r(d)$ pour d pair) le plus grand nombre premier de $P_{d,r}$ (resp. $Q_{d,r}$) si $P_{d,r} \cap \Pi$ (resp. $Q_{d,r} \cap \Pi$) est non vide, 1 sinon.

Pour d pair, on a l'inégalité évidente $\mu_r(d) \leq \lambda_r(d)$. Posons

$$\lambda(d) = \max_{0 \leq r \leq d} \lambda_r(d),$$

et pour d pair,

$$\mu(d) = \max_{0 \leq r \leq d} \mu_r(d).$$

Pour d pair, on a $\mu(d) \leq \lambda(d)$.

Dans ce paragraphe, on notera p un nombre premier impair, $\overline{\mathbb{F}}_p$ une clôture algébrique de $\mathbb{F}_p$ et pour x dans $\mathbb{F}_p$, $\varepsilon(x)$ l'entier défini par : Si $x = 0$, $\varepsilon(x) = 0$ et si x est non nul, $\varepsilon(x)$ vaut 1 (resp. -1) si x est (resp. n'est pas) un carré de $\mathbb{F}_p$.

Le lemme suivant s'inspire d'un travail de Stark [9] sur les courbes hyperelliptiques.

Lemme 1. *Soient p un nombre premier impair et f un élément non nul de $\mathbb{F}_p[X]$ de degré $d < p$. Posons $\delta = [(d+1)/2]$ et pour $k = 0, 1, -1$,*

$$f_k = \prod_{\substack{x \in \mathbb{F}_p \\ \varepsilon(f(x))=k}} (X - x).$$

Il existe un élément R de $\mathbb{F}_p[X]$ ayant les propriétés suivantes :

(i) *R est divisible par $f_0^{\delta} f_1^{\delta+1}$ et de degré $\leq \delta(d+p-1)$.*

(ii) *Si d est pair et si le coefficient dominant de f est un carré, R est de degré $\leq \delta(d+p-2)-1$.*

(iii) *Si f a un zéro simple dans $\overline{\mathbb{F}}_p$, R est non nul.*

Démonstration. Posons $K = \mathbb{F}_p((1/X))$. Soient $f^{1/2}$ une racine carré de f dans une clôture algébrique de K et D le prolongement de la dérivation de K par rapport à X à l'extension $K(f^{1/2})$. Définissons deux suites d'éléments de $\mathbb{F}_p(X)$, $(F_i)_{i \in \mathbb{N}}$ et $(r_i)_{i \in \mathbb{N}}$ par

$$F_0 = 1 - f^{(p-1)/2}, \quad F_{i+1} = DF_i + \frac{f'}{2f} F_i,$$

$$r_0 = f^{\delta}, \quad r_{i+1} = Dr_i - \frac{f'}{2f} r_i.$$

Posons

$$T = \sum_{j=0}^{\delta} \frac{1}{j!} F_j (X^p - X)^j,$$

et pour $i \geq 0$ entier,

$$R_i = T r_i.$$

Avant de montrer le lemme, on va établir quelques formules :

$$X^p - X = f_{-1} f_0 f_1. \tag{1}$$

Pour tout entier $i \geq 1$,

$$F_i = f^{-1/2} D^i (f^{1/2}). \tag{2}$$

Pour tout entier $i \geq 1$, il existe des éléments P_i et Q_i de $\mathbb{F}_p[X]$ tels que P_i soit de degré $\leq (d-1)i$ et que l'on ait

$$F_i = P_i / f^i, \tag{3}$$

$$r_i = Q_i / f^i, \tag{4}$$

$$R_0 = (1 - f^{(p-1)/2}) f^{\delta} + \sum_{j=1}^{\delta} \frac{1}{j!} P_j f^{\delta - j} (X^p - X)^j. \tag{5}$$

Pour tout entier $i \geq 0$,

$$DR_i = R_{i+1} + \frac{1}{\delta!} (X^p - X)^{\delta} r_i F_{\delta+1}. \tag{6}$$

La formule (1) est évidente, (3) et (4) s'obtiennent par récurrence et (5) résulte de (3). Pour $i \geq 1$ entier, on a

$$F_i = DF_{i-1} + \frac{f'}{2f} F_{i-1} = f^{-1/2} D(f^{1/2} F_{i-1}),$$

d'où

$$F_1 = f^{-1/2} D(f^{1/2} F_0) = f^{-1/2} D(f^{1/2} - (f^{1/2})^p) = f^{-1/2} D(f^{1/2})$$

et, par récurrence, la formule (2).

Montrons (6). On a

$$DR_i = r_i DT + T Dr_i = T r_{i+1} + \left(DT + \frac{f'}{2f} T \right) r_i,$$

$$DT + \frac{f'}{2f} T = \sum_{j=0}^{\delta} \frac{1}{j!} \left(DF_j + \frac{f'}{2f} F_j \right) (X^p - X)^j - \sum_{j=1}^{\delta} \frac{1}{(j-1)!} F_j (X^p - X)^{j-1}$$

$$= \sum_{j=0}^{\delta} \frac{1}{j!} F_{j+1}(X^p - X)^j - \sum_{j=0}^{\delta-1} \frac{1}{j!} F_{j+1}(X^p - X)^j$$
$$= \frac{1}{\delta!}(X^p - X)^\delta F_{\delta+1},$$

d'où (6).

Posons $R = R_0$ et montrons (i).

Vu (5) et (1), f_0^δ divise R. Soit x un élément de $\mathbb{F}_p$ tel que $\varepsilon(f(x)) = 1$. On a $F_0(x) = 0$, donc $T(x) = 0$, d'où pour tout entier $i \geq 0$, $R_i(x) = 0$. Il résulte alors de (4) et (6) qu'on a

$$R(x) = (DR)(x) = \ldots = (D^\delta R)(x) = 0,$$

donc $f_1^{\delta+1}$ divise R et R est divisible par $f_0^\delta f_1^{\delta+1}$.

Dans (5), le degré de chacun des termes sous le signe somme est $\leq \delta(d + p - 1)$ et comme $(1 - f^{(p-1)/2})f^\delta$ est de degré $\leq \frac{p-1}{2}d + \delta d$ et $d/2 \leq \delta$, R est de degré $\leq \delta(d + p - 1)$.

(ii) Supposons d pair. On a $\delta = d/2$. Soit a^2 le coefficient dominant de f. Posons $\pi = X^{-1}$ et notons ω la valuation π-adique sur K. Pour u, v dans K et n dans $\mathbb{Z}$, nous noterons $u \equiv v\ (\pi^n)$ le fait que $\omega(u - v) \geq n$; vu nos hypothèses, $f^{1/2}$ appartient à K et on peut supposer que $f^{1/2} = aX^\delta + g$ avec $\omega(g) \geq 1 - \delta$.

Lorsque $d = 0$, on a $R = 0$; d'où le résultat. Supposons $d \geq 2$. On a

$$F_0 f^\delta \equiv -aX^{p\delta} f^{-1/2} f^\delta\ (\pi^{-\delta(d+p-2)+1})$$

et, vu la formule (2),

$$R \equiv \left(\sum_{j=1}^{\delta} \frac{1}{j!} D^j(f^{1/2})(X^p - X)^j - aX^{p\delta} \right) f^\delta f^{-1/2}\ (\pi^{-\delta(d+p-2)+1}).$$

D'autre part, pour tout entier $j \leq \delta$, on a

$$D^j(f^{1/2}) = \frac{a\delta!}{(\delta - j)!} X^{\delta-j} + D^j(g).$$

Si $j < \delta$, on a $\omega(D^j(g)) \geq 1 + j - \delta$, et $\omega(D^\delta(g)) \geq \delta + 1$. Donc

$$R \equiv \left(a \sum_{j=1}^{\delta} \binom{\delta}{j} X^{\delta-j}(X^p - X)^j - aX^{p\delta} \right) f^\delta f^{-1/2}$$
$$\equiv -aX^\delta f^\delta f^{-1/2}\ (\pi^{-\delta(d+p-2)+1}).$$

Par suite, $\omega(R) \geq -\delta(d + p - 2) + 1$, d'où (ii).

(iii) Supposons que f ait un zéro simple dans $\overline{\mathbb{F}}_p$. Montrons qu'alors R est non nul. On raisonnera par l'absurde en supposant R nul. Puisque R est nul, T est nul et vu la formule (6) pour $i = 0$, $F_{\delta+1}$ est nul. En appliquant

$\delta+1$ fois la dérivation D à $f^{1/2}$, on obtient

$$D^{\delta+1}(f^{1/2}) = f^{1/2}\sum_{j=1}^{\delta+1} g_j f^{-j},$$

où les g_j sont dans $\mathbb{F}_p[X]$ et où

$$g_{\delta+1} = -\Big(-\frac{f'}{2}\Big)^{\delta+1}\prod_{k=0}^{\delta-1}(2k+1).$$

En tenant compte de (2) pour $i=\delta+1$, on a

$$\sum_{j=1}^{\delta+1} g_j f^{-j} = F_{\delta+1} = 0,$$

d'où

$$\sum_{j=1}^{\delta} g_j f^{\delta-j+1} = \Big(-\frac{f'}{2}\Big)^{\delta+1}\prod_{k=0}^{\delta-1}(2k+1).$$

Comme $2\delta-1 \le d$ et $d<p$, le produit $\prod_{k=0}^{\delta-1}(2k+1)$ est non nul, donc f a toutes ses racines multiples, ce qui est absurde.

LEMME 2. *Soit f un élément de $\mathbb{F}_p[X]$, non carré, de degré $d<p$, et tel que pour tout x de $\mathbb{F}_p$, $f(x)$ soit un carré de $\mathbb{F}_p$. Il existe un élément g de $\mathbb{F}_p[X]$, non carré, de même coefficient dominant que f, de degré $d' \le d$, et tel que d' et d soient de même parité, g et f aient le même nombre de zéros dans $\mathbb{F}_p$, g ait un zéro simple dans $\overline{\mathbb{F}}_p$ et que pour tout x de $\mathbb{F}_p$, $g(x)$ soit un carré de $\mathbb{F}_p$.*

Démonstration. Soit $f = aP_1^{n_1}\dots P_r^{n_r}$, la décomposition de f en polynômes irréductibles dans $\mathbb{F}_p[X]$ avec $P_1,\dots,P_r$ unitaires et distincts deux à deux. Si tous les n_i sont pairs, comme $d<p$, il existe un élément x de $\mathbb{F}_p$ tel que $f(x)$ soit non nul. Par suite, a sera un carré de $\mathbb{F}_p$ et f un carré de $\mathbb{F}_p[X]$, ce qui est absurde. Donc on peut supposer n_1 impair. Posons

$$g = aP_1P_2^{n_2}\dots P_r^{n_r}.$$

Soit x un élément de $\mathbb{F}_p$. Si $P_1(x)$ est nul, $g(x)$ est nul et si $P_1(x)$ est non nul, $g(x)$ est un carré de $\mathbb{F}_p$, donc pour tout élément x de $\mathbb{F}_p$, $g(x)$ est un carré de $\mathbb{F}_p$. Tout zéro de P_1 est un zéro simple de g et on vérifie que g satisfait aussi aux autres propriétés énoncées dans le lemme.

THÉORÈME 1. *Soient d, r deux entiers tels que $0 \le r \le d$, p un nombre premier impair tel que $p > r+(d-1)[(d+1)/2]$ et f un élément non nul de $\mathbb{F}_p[X]$, de degré d, ayant exactement r zéros dans $\mathbb{F}_p$, et tel que pour tout x de $\mathbb{F}_p$, $f(x)$ soit un carré de $\mathbb{F}_p$. Il existe alors un élément g de $\mathbb{F}_p[X]$ tel que $f=g^2$.*

Démonstration. Raisonnons par l'absurde en supposant qu'il existe un nombre premier impair p tel que $p > r + (d-1)[(d+1)/2]$ et un élément f de $\mathbb{F}_p[X]$, non carré de $\mathbb{F}_p[X]$, de degré d, ayant exactement r zéros dans $\mathbb{F}_p$, et tel que pour tout x de $\mathbb{F}_p$, $f(x)$ soit un carré de $\mathbb{F}_p$.

Nos hypothèses entraînent $d < p$. Le polynôme obtenu en appliquant le lemme 2 à f vérifie les mêmes hypothèses que f et a un zéro simple dans $\overline{\mathbb{F}}_p$, donc on peut supposer que f a un zéro simple dans $\overline{\mathbb{F}}_p$. En vertu du (i) et (iii) du lemme 1 et, avec les notations de ce lemme, il existe un élément R de $\mathbb{F}_p[X]$ non nul, divisible par $f_0^{\delta} f_1^{\delta+1}$ et de degré $\leq \delta(d+p-1)$, où $\delta = [(d+1)/2]$; f_0 et f_1 sont de degrés respectifs r et $p-r$; d'où

$$\delta r + (\delta+1)(p-r) \leq \delta(d+p-1),$$

donc $p \leq r + (d-1)[(d+1)/2]$, ce qui est absurde.

Ce théorème justifie la définition de $\lambda_r(d)$ et de $\mu_r(d)$ et on a :

Théorème 2. *Soient $d \geq 2$ et r deux entiers tels que $0 \leq r \leq d$. Alors*

$$\lambda_r(d) \leq r + (d-1)[(d+1)/2].$$

Corollaire. (i) *Pour tout entier d impair ≥ 3,*

$$\lambda_0(d) \leq (d^2-3)/2.$$

(ii) $\lambda_0(2) = 1$, $\lambda_0(4) = 5$ *et pour tout entier d pair ≥ 6,*

$$\lambda_0(d) \leq (d^2-d-4)/2.$$

(iii) *Pour tout entier $d \geq 8$ et multiple de 4,*

$$\lambda_0(d) \leq (d^2-d-10)/2.$$

Démonstration. D'aprés le théorème précédent, si $d \geq 2$,

$$\lambda_0(d) \leq (d-1)[(d+1)/2].$$

Donc si d est ≥ 3 et impair, on a $\lambda_0(d) \leq (d^2-1)/2$; et comme $\lambda_0(d)$ vaut 1 ou un nombre premier impair, $\lambda_0(d) \leq (d^2-3)/2$, d'où (i). Si d est ≥ 2 et pair, $\lambda_0(d) \leq d(d-1)/2$, donc $\lambda_0(2) = 1$ et, si $d \geq 4$, $d(d-1)/2$ n'est pas un nombre premier, donc $\lambda_0(d) \leq d(d-1)/2 - 1$, ou encore $\lambda_0(d) \leq (d+1)(d-2)/2$. En particulier, $\lambda_0(4) \leq 5$ et sur $\mathbb{F}_5$, le polynôme $3X^4+1$ ne prend que des valeurs carrées non nulles et n'est pas un carré, donc $\lambda_0(4) = 5$. Si d est ≥ 6 et pair, $(d+1)(d-2)/2$ n'est pas un nombre premier, donc $\lambda_0(d) \leq (d^2-d-4)/2$, d'où (ii). Par un raisonnement analogue à celui utilisé pour (ii), on obtient (iii).

Théorème 3. *Soit d un entier ≥ 2.*

(i) *Si d est impair*,

$$\lambda(d) \leq (d^2+2d-1)/2.$$

(ii) $\lambda(2) = \lambda_2(2) = 3$ *et si* $d \geq 4$ *est pair*,

$$\lambda(d) \leq (d^2 + d - 4)/2.$$

(iii) $\lambda(4) = \lambda_4(4) = 7$ *et si* $d \geq 8$ *est multiple de* 4,

$$\lambda(d) \leq (d^2 + d - 10)/2.$$

Démonstration. Vu le théorème 2, on a

$$\lambda(d) \leq d + (d-1)[(d+1)/2],$$

d'où (i). Si d est ≥ 2 et pair, $\lambda(d) \leq d(d+1)/2$, donc si $d \geq 6$, les résultats du (ii) et (iii) sont les conséquences du fait que $\lambda(d)$ vaut 1 ou un nombre premier impair. Si $d = 2$, $\lambda(2) \leq 3$ et sur $\mathbb{F}_3$, le polynôme $2(X^2 - 1)$ ne prend que des valeurs carrées et n'est pas un carré, donc $\lambda(2) = \lambda_2(2) = 3$. Si $d = 4$, $\lambda(4) \leq 10$ et sur $\mathbb{F}_7$, le polynôme $X^4 + X = X(X^3 + 1)$ ne prend que des valeurs carrées et n'est pas carré, donc $\lambda(4) = \lambda_4(4) = 7$; d'où (ii) et (iii).

Théorème 4. *Soient* $d \geq 0$ *un entier pair*, r *un entier tel que* $0 \leq r \leq d$, p *un nombre premier impair tel que* $p > r + (d^2 - 2d - 2)/2$ *et* f *un élément non nul de* $\mathbb{F}_p[X]$, *de coefficient dominant carré de* $\mathbb{F}_p$, *de degré* d, *ayant exactement* r *zéros dans* $\mathbb{F}_p$, *et tel que pour tout* x *de* $\mathbb{F}_p$, $f(x)$ *soit un carré de* $\mathbb{F}_p$, *il existe alors un élément* g *de* $\mathbb{F}_p[X]$ *tel que* $f = g^2$.

Démonstration. Raisonnons par l'absurde en supposant qu'il existe un nombre premier impair p tel que $p > r + (d^2 - 2d - 2)/2$ et un élément f de $\mathbb{F}_p[X]$, non carré de $\mathbb{F}_p[X]$, de coefficient dominant carré de $\mathbb{F}_p$, de degré d pair, ayant exactement r zéros dans $\mathbb{F}_p$, et tel que pour tout x de $\mathbb{F}_p$, $f(x)$ soit un carré de $\mathbb{F}_p$.

Nos hypothèses entraînent $d < p$. En appliquant le lemme 2, on peut supposer que f a un zéro simple dans $\overline{\mathbb{F}}_p$ et d'après le lemme 1, et avec les notations de ce lemme, il existe un polynôme R de $\mathbb{F}_p[X]$ non nul, divisible par $f_0^{\delta} f_1^{\delta+1}$ et de degré $\leq \delta(d + p - 2) - 1$, où $\delta = d/2$; f_0 et f_1 sont de degrés respectifs r et $p - r$; d'où

$$\delta r + (\delta + 1)(p - r) \leq \delta(d + p - 2) - 1,$$

donc $p \leq r + (d^2 - 2d - 2)/2$, ce qui est absurde.

On a les conséquences immédiates suivantes de ce théorème :

Théorème 5. (i) *Pour tout* r, $\mu_r(2) = 1$.

(ii) *Pour tout entier pair* $d \geq 4$ *et tout entier* r *tels que* $0 \leq r \leq d$,

$$\mu_r(d) \leq r + (d^2 - 2d - 2)/2.$$

(iii) *Pour tout entier pair* $d \geq 2$,

$$\mu(d) \leq (d^2 - 2)/2.$$

Avant de donner quelques valeurs numériques, citons les résultats suivants qui les justifieront : Les polynômes $f_1 = 2(X^2-1)$ sur $\mathbb{F}_3$, $f_2 = X^3+1$ et $f_3 = X^4 + X$ sur $\mathbb{F}_7$, $f_4 = 3(X+1)(X+3)(X+6)(X-6)(X-8)$ et $f_5 = X(X+1)(X+2)(X+3)(X-3)(X+6)$ sur $\mathbb{F}_{17}$ ne prennent que des valeurs carrées et ne sont pas des carrés. Pour le calcul de $\lambda(6)$, le théorème 3 donne $\lambda(6) \leq 19$ et un calcul sur machine a montré que $\lambda(6) < 19$.

d	$\lambda(d)$	$(d^2+d-4)/2$	$\mu(d)$	$(d^2-2)/2$
2	3	1	1	1
4	7	8	7	7
6	17	19	17	17

d	$\lambda(d)$	$(d^2+2d-1)/2$
3	7	7
5	17	17

Le théorème suivant montre que les fonctions μ_0, λ_0, μ et λ ne peuvent être majorées par une fonction linéaire.

THÉORÈME 6. *Si u est l'une des fonctions μ_0, λ_0, μ, λ, on a*

$$\limsup \frac{u(d)}{d} = \infty.$$

D é m o n s t r a t i o n. Il suffit de montrer le théorème pour $u = \mu_0$. Soit n un entier ≥ 1. D'après le théorème de Dirichlet, il existe une suite infinie d'entiers pairs strictement croissante $(d_k)_{k\in\mathbb{N}}$ telle que pour tout $k \geq 0$, $p_k = nd_k + 1$ soit un nombre premier. Pour $k \geq 0$, soient $a_1, \ldots, a_n$ les puissances d_k-ièmes des éléments non nuls de $\mathbb{F}_{p_k}$. Considérons le système d'équations suivant :

$$y_1^2 = x + a_1, \ \ldots, \ y_n^2 = x + a_n \quad \text{et} \quad y_{n+1}^2 = x.$$

Vu le théorème 5A de la page 52 de [8], il existe un entier k_0 et un réel $c > 0$ tels que si $k \geq k_0$ et si N est le nombre de solutions $(x, y_1, \ldots, y_{n+1})$ de ce système dans $\mathbb{F}_{p_k}^{n+2}$, on a

$$|N - p_k| < c\sqrt{p_k}.$$

Le nombre de solutions $(x, y_1, \ldots, y_{n+1})$ telles que x ou l'un des y_i soit nul est au plus égal à $(n+1)2^n$. Donc pour k assez grand, le système en question a une solution $(a, b_1, \ldots, b_{n+1})$ telle que $a, b_1, \ldots, b_{n+1}$ sont tous des éléments non nuls de $\mathbb{F}_{p_k}$; pour un tel entier k, notons d l'entier d_k, p le nombre premier $nd+1$ et considérons l'élément $f = X^d + a$ de $\mathbb{F}_p[X]$. On a $f(0) = a = b_{n+1}^2$ et, si x est un élément non nul de $\mathbb{F}_p$ et si i est tel que $x^d = a_i$, $f(x) = a_i + a = b_i^2$. Donc f ne prend que des valeurs carrées non nulles de $\mathbb{F}_p$; de plus f est unitaire, sans racines dans $\mathbb{F}_p$ et n'est pas un carré de $\mathbb{F}_p[X]$, donc $\mu_0(d) \geq nd+1$, d'où le théorème.

3. Le cas général. Introduisons la définition suivante que nous justifierons ci-dessous.

DÉFINITION. Soient $d \geq 2$ et r deux entiers tels que $0 \leq r \leq d$. Nous noterons $\Lambda_r(d)$ (resp. $M_r(d)$ pour d pair) le plus grand élément de $P_{d,r}$ (resp. $Q_{d,r}$) si $P_{d,r}$ (resp. $Q_{d,r}$) est non vide, 1 sinon.

On a les inégalités évidentes : $\lambda_r(d) \leq \Lambda_r(d)$, et pour d pair, $\mu_r(d) \leq M_r(d)$ et $M_r(d) \leq \Lambda_r(d)$. Posons

$$\Lambda(d) = \max_{0 \leq r \leq d} \Lambda_r(d),$$

et pour d pair,

$$M(d) = \max_{0 \leq r \leq d} M_r(d).$$

On a $\lambda(d) \leq \Lambda(d)$, et pour d pair, $\mu(d) \leq M(d)$ et $M(d) \leq \Lambda(d)$.

THÉORÈME 7. *Soient $d \geq 2$ et r deux entiers tels que $0 \leq r \leq d$.*

(i) *Si d est impair*,

$$\Lambda_r(d) \leq \left(\frac{d-1}{2} + \sqrt{\left(\frac{d-1}{2}\right)^2 + r} \right)^2.$$

(ii) *Si d est pair*,

$$\Lambda_r(d) \leq \left(\frac{d-2}{2} + \sqrt{\left(\frac{d-2}{2}\right)^2 + r + 1} \right)^2.$$

(iii) *Pour tout r, $M_r(2) = 1$ et si $d \geq 4$ est pair*,

$$M_r(d) \leq \left(\frac{d-2}{2} + \sqrt{\left(\frac{d-2}{2}\right)^2 + r - 1} \right)^2.$$

Démonstration. Soient $q \geq 3$ une puissance d'un nombre premier impair et f un élément de $\mathbb{F}_q[X]$, non carré, de degré $d \geq 2$, ayant exactement r zéros dans $\mathbb{F}_q$, et tel que pour tout x de $\mathbb{F}_q$, $f(x)$ soit un carré de $\mathbb{F}_q$.

Soit g le polynôme unitaire de $\mathbb{F}_q[X]$ de degré maximal tel que $f = g^2 h$, où h est un élément de $\mathbb{F}_q[X]$. Notons n_0 le nombre de zéros de h dans $\mathbb{F}_q$ et n_1 (resp. n_{-1}) le nombre d'éléments x de $\mathbb{F}_q$ tel que $h(x)$ soit un carré non nul (resp. ne soit pas un carré) de $\mathbb{F}_q$. On a $n_0 + n_1 + n_{-1} = q$. Soit N le nombre d'éléments (x, y) de $\mathbb{F}_q \times \mathbb{F}_q$ tel que $y^2 = h(x)$. On a $N = 2n_1 + n_0$. Notons C un modèle lisse sur $\overline{\mathbb{F}}_q$ de la fermeture dans $\mathbb{P}^2$ de la courbe affine $y^2 = h(x)$, $N(C)$ le nombre de ses points $\mathbb{F}_q$-rationnels et s le nombre de ses points à l'infini définis sur $\mathbb{F}_q$. Vu les résultats ci-dessus,

$$N(C) = N + s = 2q + s - n_0 - 2n_{-1}.$$

En appliquant le théorème de Weil [10] à la courbe C, on a

$$N(C) - (q+1) \leq 2g_C\sqrt{q},$$

où $g_C = [(d^\circ(h) - 1)/2]$ est le genre de C.

D'autre part, si x est un élément de $\mathbb{F}_q$ tel que $h(x)$ n'est pas un carré de $\mathbb{F}_q$, $g(x) = 0$, donc $d^\circ(g) \geq n_{-1}$. On a $g_C = [(d-1)/2] - d^\circ(g)$, donc $g_C \leq [(d-1)/2] - n_{-1}$, d'où

$$q + s - n_0 - 1 + 2(\sqrt{q} - 1)n_{-1} \leq 2[(d-1)/2]\sqrt{q},$$

et comme $n_0 \leq r$, on a $q + s - r - 1 \leq 2[(d-1)/2]\sqrt{q}$, ce qui entraîne $[(d-1)/2]^2 + r + 1 - s \geq 0$ et

$$q \leq \left(\left[\frac{d-1}{2} \right] + \sqrt{\left[\frac{d-1}{2} \right]^2 + r + 1 - s} \right)^2.$$

Si d est impair, s vaut 1, d'où (i). Si d est pair et si le coefficient dominant de f est (resp. n'est pas) un carré, s vaut 2 (resp. 0); d'où (ii) et (iii).

THÉORÈME 8. *Soit d un entier ≥ 2.*

(i) $\Lambda_0(3) = 3$ *et si* $d \geq 5$ *est impair*, $\Lambda_0(d) \leq d^2 - 2d - 2$.
(ii) $\Lambda_0(2) = 1$, $\Lambda_0(4) = 5$ *et si* $d \geq 6$ *est pair*, $\Lambda_0(d) \leq d^2 - 4d + 1$.
(iii) $M_0(2) = 1$ *et si* $d \geq 4$ *est pair*, $M_0(d) \leq d^2 - 4d + 1$.

Démonstration. (i) Vu le théorème 7 et la parité de $\Lambda_0(d)$, on a $\Lambda_0(d) \leq d(d-2)$. Par suite, $\Lambda_0(3) \leq 3$, et sur $\mathbb{F}_3$, le polynôme $X^3 - X + 1$ ne prend que des valeurs carrées non nulles, donc $\Lambda_0(3) = 3$. Si $d \geq 5$ est impair, $d(d-2)$ ne peut être une puissance d'un nombre premier impair, donc $\Lambda_0(d) \leq d^2 - 2d - 1$, et vu la parité de $\Lambda_0(d)$, on a $\Lambda_0(d) \leq d^2 - 2d - 2$.

(ii) Pour $d \geq 2$ et pair et, vu le théorème 7, on a

$$\Lambda_0(d) \leq \frac{1}{2}d^2 - 2d + 3 + \frac{d-2}{2}\sqrt{d^2 - 4d + 8},$$

ce qui entraîne $\Lambda_0(d) \leq d^2 - 4d + 6$, et comme $\Lambda_0(d)$ est impair, $\Lambda_0(d) \leq d^2 - 4d + 5$. Par suite, $\Lambda_0(2) = 1$. On a $\Lambda_0(4) \leq 5$, et comme on a vu ci-dessus que $\lambda_0(4) = 5$, il vient $\Lambda_0(4) = 5$.

Supposons qu'il existe $d \geq 6$ et pair tel que $\Lambda_0(d) = d^2 - 4d + 5$; dans ce cas $\Lambda_0(d)$ ne peut être un nombre premier car on aurait $\Lambda_0(d) = \lambda_0(d)$; d'où, vu le corollaire du théorème 2, $d^2 - 4d + 5 \leq (d^2 - d - 4)/2$, ce qui est impossible. Donc il existe un entier $n > 1$ et un nombre premier $p \geq 3$ tels que $p^n = d^2 - 4d + 5$, ou encore $p^n = (d-2)^2 + 1$, ce qui est impossible vu le théorème de Lebesgue relatif à l'équation diophantienne $x^n = y^2 + 1$; voir par exemple [7], théorème 3.1, p. 109.

Donc $\Lambda_0(d) \leq (d-2)^2$, et vu la parité de $\Lambda_0(d)$, on a $\Lambda_0(d) \leq (d-2)^2 - 1$. Si $d \geq 6$ est pair, $(d-2)^2 - 1$ ne peut être une puissance d'un nombre premier impair, donc $\Lambda_0(d) \leq (d-2)^2 - 2$, d'où $\Lambda_0(d) \leq (d-2)^2 - 3$.

(iii) résulte du (iii) du théorème 7 si $d = 4$ et du (ii) pour les autres valeurs de d, vu que pour d pair $M_0(d) \leq \Lambda_0(d)$.

THÉORÈME 9. *Soit d un entier ≥ 2.*

(i) *Si d est impair, $\Lambda(d) \leq d^2$.*
(ii) *$\Lambda(2) = \Lambda_2(2) = 3$ et si $d \geq 4$ est pair, $\Lambda(d) \leq (d-1)^2$.*
(iii) *Si d est pair, $M(d) \leq (d-1)^2$.*

Démonstration. (i) résulte du (i) du théorème 7.
(ii) Pour $d \geq 2$ et pair et, vu le (ii) du théorème 7, on a

$$\Lambda(d) \leq \frac{1}{2}d^2 - d + 3 + \frac{d-2}{2}\sqrt{d^2+8},$$

ce qui entraîne $\Lambda(d) \leq d^2 - 2d + 4$, et en tenant compte de la parité de $\Lambda(d)$, on a $\Lambda(d) \leq d^2 - 2d + 3$. D'où $\Lambda(2) \leq 3$, et comme on a vu ci-dessus que $\lambda(2) = 3$, il en résulte que $\Lambda(2) = 3$.

Supposons qu'il existe $d \geq 4$ et pair tel que $\Lambda(d) = d^2 - 2d + 3$; dans ce cas $\Lambda(d)$ ne peut être un nombre premier car on aurait $\Lambda(d) = \lambda(d)$; d'où, vu le théorème 3, $d^2 - 2d + 3 \leq (d^2 + d - 4)/2$, ce qui est impossible. Donc il existe un entier $n > 1$ et un nombre premier $p \geq 3$ tels que $p^n = d^2 - 2d + 3$, ou encore $p^n = (d-1)^2 + 2$; or d'après [5] et [6], la seule solution en entiers (n, x, y) telle que $n > 1$ et $y > 0$ de l'équation $x^n = y^2 + 2$ est $(n, x, y) = (3, 3, 5)$, d'où $n = 3$, $p = 3$ et $d = 6$. Donc il existe un élément f de $\mathbb{F}_{27}[X]$, non carré, de degré 6 et qui ne prend que des valeurs carrées dans $\mathbb{F}_{27}$. Soit r_0 le nombre de zéros de f dans $\mathbb{F}_{27}$. En vertu du (ii) du théorème 7, si r est un entier tel que $0 \leq r \leq 5$, on a $\Lambda_r(6) < 27$, donc $r_0 = 6$; un calcul sur machine a montré qu'il n'existe pas de polynôme sur $\mathbb{F}_{27}$ de degré 6, ayant 6 zéros dans $\mathbb{F}_{27}$ et qui ne prend que des valeurs carrées dans $\mathbb{F}_{27}$, d'où une contradiction.

Donc finalement si $d \geq 4$ est pair, $\Lambda(d) \leq d^2 - 2d + 2$, et en tenant compte de la parité de $\Lambda(d)$, on a $\Lambda(d) \leq (d-1)^2$.

(iii) Le (iii) du théorème 7 entraîne $M(2) = 1$, et pour $d \geq 4$ et pair, on a $M(d) \leq \Lambda(d)$, donc $M(d) \leq (d-1)^2$.

Le théorème suivant montre que les majorations obtenues dans le théorème 9 ne peuvent en général être améliorées.

THÉORÈME 10. *Soit $q \geq 3$ une puissance d'un nombre premier impair.*

(i) *$\Lambda(q) = \Lambda_q(q) = q^2$.*
(ii) *$\Lambda(q+1) = \Lambda_{q+1}(q+1) = q^2$.*
(iii) *$M(q+1) = M_{q+1}(q+1) = q^2$.*
(iv) *Si $q \equiv 1 \pmod 3$, on a $M_0(2q-2) \geq q^2$ et $\Lambda_0(2q-2) \geq q^2$.*

Démonstration. (i) Considérons le polynôme $f = X^q + X$ sur $\mathbb{F}_{q^2}$ et soit x un élément de $\mathbb{F}_{q^2}$. On a $f(x)^q = f(x)$, donc $f(x)$ est un carré de $\mathbb{F}_{q^2}$; de plus, on remarque que f a q racines distinctes dans $\mathbb{F}_{q^2}$, donc $\Lambda(q) \geq \Lambda_q(q) \geq q^2$, et vu le théorème 9, $\Lambda(q) = \Lambda_q(q) = q^2$.

(ii) et (iii). Considérons l'élément $f = X^{q+1} - 1$ de $\mathbb{F}_{q^2}[X]$ et soit x un élément de $\mathbb{F}_{q^2}$. On a $f(x)^q = f(x)$, donc $f(x)$ est un carré de $\mathbb{F}_{q^2}$. Le polynôme f est unitaire et a exactement $q+1$ racines dans $\mathbb{F}_{q^2}$, donc $\Lambda(q+1) \geq \Lambda_{q+1}(q+1) \geq q^2$ et $M(q+1) \geq M_{q+1}(q+1) \geq q^2$, et vu le théorème 9, $\Lambda(q+1) = \Lambda_{q+1}(q+1) = q^2$ et $M(q+1) = M_{q+1}(q+1) = q^2$.

(iv) Supposons $q \equiv 1 \pmod 3$ et considérons l'élément $f = X^{2q-2} - X^{q-1} + 1$ de $\mathbb{F}_{q^2}[X]$. Soit x une racine non nulle de f' dans une clôture algébrique de $\mathbb{F}_{q^2}$. On a $x^{q-1} = 1/2$, donc $f(x) = 3/4$. Donc f n'a que des racines simples et par suite, il n'est pas un carré. Montrons que f ne prend que des valeurs carrées dans $\mathbb{F}_{q^2}$. Soit x un élément de $\mathbb{F}_{q^2}$. On a $(x^2 f(x))^q = x^2 f(x)$, donc $x^2 f(x)$ est un carré de $\mathbb{F}_{q^2}$ et $f(x)$ est un carré de $\mathbb{F}_{q^2}$. Montrons enfin que f n'a pas de racine dans $\mathbb{F}_{q^2}$. Supposons qu'il existe un élément x de $\mathbb{F}_{q^2}$ tel que $f(x) = 0$ et posons $\alpha = x^{q-1}$. On a $\alpha^{q+1} = 1$. D'autre part, $\alpha^2 - \alpha + 1 = 0$, d'où $\alpha^3 = -1$, donc α est d'ordre 6 dans le groupe multiplicatif des éléments non nuls de $\mathbb{F}_{q^2}$, ce qui est absurde. Donc $M_0(2q-2) \geq q^2$ et $\Lambda_0(2q-2) \geq q^2$.

Bibliographie

[1] L. Carlitz, *A problem of Dickson's*, Duke Math. J. 14 (1947), 1139–1140.

[2] —, *A problem of Dickson*, ibid. 19 (1952), 471–474.

[3] —, *Note on a problem of Dickson*, Proc. Amer. Math. Soc. 14 (1963), 98–100.

[4] L. E. Dickson, *Definite forms in a finite field*, Trans. Amer. Math. Soc. 10 (1909), 109–122.

[5] W. Ljunggren, *Über einige Arcustangensgleichungen die auf interessante unbestimmte Gleichungen führen*, Ark. Mat. Astr. Fys. 29A (1943), no. 13, 11 pp.

[6] T. Nagell, *Verallgemeinerung eines Fermatschen Satzes*, Arch. Math. (Basel) 5 (1954), 153–159.

[7] W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientific Publishers, Warszawa, 1986.

[8] W. M. Schmidt, *Equations over Finite Fields. An Elementary Approach*, Lecture Notes in Math. 536, Springer, 1976.

[9] H. M. Stark, *On the Riemann hypothesis in hyperelliptic function fields*, in: Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 285–302.

[10] A. Weil, *Variétés abéliennes et courbes algébriques*, Hermann, Paris, 1948.

DÉPARTEMENT DE MATHÉMATIQUES APPLIQUÉES ET INFORMATIQUE
FACULTÉ DES SCIENCES ET TECHNIQUES
UNIVERSITÉ CADI AYYAD
B.P. 71
BENI-MELLAL, MAROC

Reçu le 30.4.1993
et révisé le 17.4.1994 (2425)