QUADRATIC RESIDUES IN $_q[T]$

Mireille CAR

Laboratoire de Mathématiques
Bâtiment Henri Poincaré
Faculté des Sciences de Saint-Jérôme
Avenue Escadrille Normandie-Niemen
13397 MARSEILLE Cedex 20
FRANCE

Email : mireille.car@math.u-3mrs.fr

Let q be a power of an odd prime number. For $H \in {}_q[T]$ a non constant polynomial, let $N(H)$, respectively $R(H)$, denote the smallest integer k such that for every polynomial $A \in {}_q[T]$ coprime with H, there exists $X \in {}_q[T]$, a monic, respectively a monic irreducible, polynomial of degree k, coprime with H, such that AX is a square modulo H. We give an upper bound for the numbers $R(H)$ from which one may deduce an upper bound for the numbers $N(H)$. This bound is given by the following theorem.

THEOREM 1 - *For any non-constant polynomial $H \in {}_q[T]$, one has*

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

This theorem admits the following corollary which shows that $R(H)/degH$ tends to 0 when $degH$ tends to $+\infty$.

COROLLARY - *Let $H \in [T]$ be such that $degH \geq 2$. Then, one has*

$$R(H) \leq C(q)\frac{degH}{log(degH)},$$

where

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

In the case where H is an irreducible polynomial we obtain the following result.

THEOREM 2 - (1) *For any irreducible polynomial* $P \in {}_q[T]$, *one has*

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

(2) *There exists an integer* $\delta(q)$ *such that for any irreducible polynomial* $P \in {}_q[T]$ *with degree*$\geq \delta(q)$, *one has*

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

Moreover, $\delta(3) = 5$, $\delta(5) = \delta(7) = 4$, $\delta(9) = 3$, *and* $\delta(q) = 2$ *for any* $q \geq 11$.

(3) *Let* d *be a positive integer such that* $q > (d-1)^2$. *Then, for any irreducible polynomial* $P \in {}_q[T]$ *of degree* d, *one has* $R(P) = 1$.