Université d'Aix-Marseille II - Luminy

Examen Master 2 M.D.F.I.
Algèbre, Arithmétique et Codage
Mars 2007
Durée : 3 heures

1. Borne de Carlitz-Uchiyama

1. Soit $q = p^m$ $(m \geq 1)$ une puissance d'un nombre premier p. Si α est un élément du corps fini $\mathbb{F}_q$, on définit sa trace sur $\mathbb{F}_p$, notée $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$, ou plus simplement $Tr(\alpha)$, par :

$$Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}.$$

1.1. Montrer que pour tout α et β dans $\mathbb{F}_q$, on a :

(i) $Tr(\alpha) \in \mathbb{F}_p$.
(ii) $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$.
(iii) $Tr(\alpha^p) = Tr(\alpha)$.

1.2. Montrer que pour $\alpha \in \mathbb{F}_q$, on a $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$ si et seulement s'il existe $\beta \in \mathbb{F}_q$ tel que $\alpha = \beta^p - \beta$ (Théorème 90 de Hilbert).
(On pourra considérer une racine β du polynôme $x^p - x - \alpha$ dans une extension de $\mathbb{F}_q$.)

2. On considère un polynôme $f(x)$ de $\mathbb{F}_q[x]$ de degré 3 avec q une puissance de 2 et on s'intéresse à la somme suivante :

$$S(f) = \sum_{x \in \mathbb{F}_q} (-1)^{Tr_{\mathbb{F}_q/\mathbb{F}_2}(f(x))}.$$

On considère la courbe algébrique affine $\mathcal{C}$ d'équation :

$$y^2 - y = f(x)$$

et l'on note N le nombre de points rationnels sur $\mathbb{F}_q$ de la clôture projective $\overline{\mathcal{C}}$ de $\mathcal{C}$.

2.1. Montrer que $\overline{\mathcal{C}}$ n'admet qu'un seul point à l'infini et que

$$N - 1 = 2 \,.\, \sharp\{x \in \mathbb{F}_q \mid Tr_{\mathbb{F}_q/\mathbb{F}_2}(f(x)) = 0\}.$$

En déduire que :

$$S(f) = N - q - 1.$$

2.2. Montrer que la courbe $\overline{\mathcal{C}}$ est non singulière.

En déduire que l'on a (borne de Carlitz-Uchiyama) :

$$\mid S(f) \mid \leq 2\sqrt{q}.$$

2. Calculs explicites

Soit μ le caractère additif canonique d'un corps fini L d'ordre 2^m. On considère Q la fonction booléenne définie sur L par $Q(x) = \mathrm{Tr}_L(x^3)$ où Tr_L désigne la trace de L sur $\mathbf{F}_2$. Le coefficient de Fourier de Q en $a \in L$ est :

$$\widehat{Q}(a) = \sum_{x \in L} \mu(x^3 + ax)$$

(1) Soient σ_1, σ_2, ..., σ_n des automorphismes distincts de L. Soient a_1,a_2,...,a_m des éléments de L, montrer que $\sum_{i=1} a_i\sigma_i = 0$ si et seulement si $a_1 = a_2 = \ldots = a_m = 0$.

(2) Montrer que la forme bilinéaire $(x, y) \mapsto \phi(x, y) = \mathrm{Tr}_L(xy)$ est non dégénérée.

(3) Préciser la nature de l'application ψ définie par

$$\forall x, y \in L, \quad Q(x + y) = Q(x) + Q(y) + \psi(x, y)$$

En déduire que Q est une forme quadratique sur $\mathbf{F}_2$, puis calculer la dimension du radical (ou noyau) de Q i.e. l'ensemble $\{x \in L \mid \forall y \in L, \quad \psi(x, y) = 0\}$.

(4) Déduire de la question précédente le spectre de Fourier de Q, en fonction de la parité de m. (indication : calculer le carré des coefficients de Fourier).

À partir de maintenant, on suppose m impair.

(5) Montrer que $x \mapsto x^2$ et $x \mapsto x^3$ sont deux permutations de L. On notera $x \mapsto \sqrt{x}$ et $x \mapsto \sqrt[3]{x}$ les permutations réciproques correspondantes.

(6) Soit $f(x) = Ax^3 + Bx^2 + Cx + D$ où $0 \neq A$, B, C et D désignent des éléments du corps L. Montrer que

$$S(f) = \mu(D)\, \widehat{Q}\Big(\frac{\sqrt{B} + C}{\sqrt[3]{A}}\Big)$$

où $S(f)$ est la somme exponentielle définie dans la première partie.

(7) Calculer $\widehat{Q}(1)$ quand $m = 1$.

(8) On suppose m premier impair. Montrer que

$$\widehat{Q}(1) \equiv 2 \mod m$$

en déduire que

$$\widehat{Q}(1) = \left(\frac{2}{m}\right) 2^{\frac{m+1}{2}}$$

où $\left(\frac{2}{m}\right)$ désigne le caractère quadratique modulo m. On rappelle que $\left(\frac{2}{m}\right) \equiv 2^{\frac{m-1}{2}} \pmod m$