Université Pierre et Marie Curie LICENCE A Année 2005-2006

Devoir 2

Exercice 1. ***Formes quadratiques non dégénérées*** *On suppose ici $p \neq 2$ et on considère une forme quadratique Q sur $\mathbb{F}_q$ en n variables non dégénérée.*

(i) Montrer que quitte à effectuer un changement de base on peut se ramener à $Q'(y) = a_1 y_1^2 + \cdots + a_n y_n^2$ avec $\left(\frac{D_Q}{p}\right) = \left(\frac{D_{Q'}}{p}\right)$ où D_Q est le discriminant de Q.

(ii) On introduit les sommes de Gauss

$$\tau(a) = \sum_{x=0}^{p-1} \exp(\frac{2i\pi a x^2}{p})$$

Montrer que $\tau(a) = (\frac{a}{p})\tau(1)$ puis que $\tau(a)$ est la somme de Gauss introduite dans le cours, i.e. $\sum_{x\in\mathbb{F}_p} (\frac{x}{p}) \exp(\frac{2i\pi a x}{p})$

(iii) Soit N_p le nombre de solutions dans $\mathbb{F}_p^n$ de $Q(x) = 0$. En écrivant

$$pN_p = \sum_{a=0}^{p-1} \sum_{x\in\mathbb{F}_p} \exp(\frac{2i\pi Q(x)}{p})$$

montrer que $N_p = p^{n-1} + \epsilon(p-1)p^{\frac{n}{2}-1}$ avec

$$\epsilon = \begin{cases} 0 \text{ si } n \equiv 1 \mod 2 \\ \left(\frac{(-1)^{n/2} D_Q}{p}\right) \text{ si } n \equiv 0 \mod 2 \end{cases}$$

(iv) Soit désormais pour $m \geq 2$

$$N_{p^m} = \text{card}\mathcal{C}_Q(p^m) \qquad \mathcal{C}_Q(p^m) := \{x \mod p^m \ / \ Q(x) \equiv 0 \mod p^m \text{ et } x \not\equiv 0 \mod p\}$$

Montrer que $N_{p^m} = p^{(m-1)(n-1)} N_p$.

(v) Comment calculer le nombre de solutions modulo N de l'équation $Q(x) \equiv 0 \mod N$?

Preuve : (i) On écrit $X(x) = {}^t x A x$ où A est une matrice symétrique, qui est donc diagonalisable dans une base (e_i). Si on note y le vecteur dans cette nouvelle base, on a $Q'(y) = a_1 y_1^2 + \cdots + a_n y_n^2$ avec $D_{Q'} = (\det P)^2 D_Q$ où P est la matrice de passage de la nouvelle base à l'ancienne de sorte que $\left(\frac{D_Q}{p}\right) = \left(\frac{D_{Q'}}{p}\right)$.

(ii) Soit a un résidu quadratique modulo p, et b un non résidu quadratique modulo p. On a

$$\tau(a) + \tau(b) = \sum_{x=0}^{p-1} \exp(\frac{2i\pi a x^2}{p}) + \sum_{x=0}^{p-1} \exp(\frac{2i\pi a x^2}{p}) = 2 + 2 \sum_{u\in a\mathbb{F}_p^{*2}} \exp(\frac{2i\pi u}{p}) + 2 \sum_{u\in b\mathbb{F}_p^{*2}} \exp(\frac{2i\pi u}{p}) = 0$$

de sorte que $\tau(a) = \tau(1)$ et $\tau(b) = -\tau(1)$.

Remarquons que $1 + \left(\frac{x}{p}\right)$ est égal au nombre de solutions de $y^2 = x$. On en déduit

$$\sum_{x\in\mathbb{F}_p} (\frac{x}{p}) \exp(\frac{2i\pi a x}{p}) = \sum_{x\in\mathbb{F}_p} (1 + (\frac{x}{p})) \exp(\frac{2i\pi a x}{p}) = \sum_{x=0}^{p-1} \exp(\frac{2i\pi a x^2}{p}) = \tau(a)$$

(iii) On a

$$\begin{aligned} pN_p &= \sum_{a=0}^{p-1} \sum_{x\in\mathbb{F}_p^n} \exp(\tfrac{2i\pi aQ(x)}{p}) \\ &= p^n + \sum_{a=1}^{p-1} \sum_{x\in\mathbb{F}_p^n} \exp(\tfrac{2i\pi aQ(x)}{p}) \\ &= p^n + \sum_{a=1}^{p-1} \sum_{x_1,\cdots,x_n\in\mathbb{F}_p} \exp(\tfrac{2i\pi a(a_1x_1^2+\cdots+a_nx_n^2)}{p}) \\ &= p^n + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \sum_{x_j\in\mathbb{F}_p} \exp(\tfrac{2i\pi aa_jx_j^2}{p}) = p^p + \sum_{a=1}^{p-1} \prod_{j=1}^{n} \tau(aa_j) \\ &= p^n + \tau(1)^n \left(\tfrac{a_1\cdots a_n}{p}\right) \sum_{a=1}^{p-1} \left(\tfrac{a}{p}\right)^n. \end{aligned}$$

Or $a_1\cdots a_n = D_Q$ et la somme $\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)^n$ vaut 0 (resp. $p-1$) si n est impair (resp. si n est pair). On en tire déjà $N = p^{n-1}$ si n est impair. Si n est pair, on remarque que

$$\tau(1)^n = (\tau(1)^2)^{n/2} = \left(\frac{-1}{p}\right)^{n/2} p^{n/2}$$

et on obtient bien la formule annoncée pour N_p.

(iv) On a une application évidente de $\mathcal{C}_Q(p^{m+1})$ vers $\mathcal{C}_Q(p^m)$ qui à un n-uplet d'entiers modulo p^{p+1} associe le même n-uplets d'entiers modulo p^m. Il suffit alors de montrer que cette application est surjective et que chaque fibre est de cardinal p^{n-1} car alors $N_{P^{m+1}} = p^{n-1}N_{p^m}$ et le résultat en découle. Soit donc un n-uplet d'entiers x_0 tel que $Q(x_0) = 0 \mod p^m$ ou encore tel que $Q(x) = p^m a_0$. On remarque que

$$Q(x_0 + p^m z) = Q(x_0) + 2p^m B(x_0, z) + p^{2m}Q(z) \equiv p^m(a_0 + 2B(x_0, z)) \mod p^{m+1}$$

où B est la forme bilinéaire associée à Q. Le terme est donc nul si et seulement si

$$a_0 + 2B(x_0, z) \equiv 0 \mod p.$$

Comme $x_0 \neq 0 \mod p$ et que B est non dégénérée par hypothèse, cette équation est celle d'un hyperplan affine dans $\mathbb{F}_p^n$, ce qui donne exactement p^{n-1} solutions modulo p pour z.

(v) Par application du lemme chinois la fonction qui à N associe le nombre de solutions de $Q(x) = 0$ modulo N est multiplicative, i.e. $f(MN) = f(M)f(N)$ pour tout N, M premiers entre eux.