Université d'Orléans-Tours
Département de Mathématiques
M2MA

17 octobre 2017

Problème n^0 2

On suppose que p est un nombre premier distinct de 2. On rappelle la définition du symbole de Legendre $\left(\frac{a}{p}\right)$ où a est un entier non divisible par p : il vaut 1 ou -1 selon que a est ou n'est pas un carré modulo p. On rappelle aussi que

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \qquad \text{modulo } p.$$

On note $K = \mathbf{F}_p$ le corps à p éléments.

I. Etude d'une forme quadratique

On se donne un entier impair $n = 2m + 1$ (où $m \geq 1$) et on considère la forme quadratique Q sur l'espace vectoriel K^n définie par

$$Q(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2.$$

L'objet de cette partie est de calculer le nombre $N(p, n)$ de solutions dans K^n de l'équation $Q(x) = 1$.

1) Montrer que si a et b sont des éléments non nuls de K, il existe x et y dans K tels que $ax^2 + by^2 = 1$.

2) Montrer que si a, b et c sont des éléments non nuls de K, il existe (x, y, z) dans K^3 distinct de $(0, 0, 0)$ tel que $ax^2 + by^2 + cz^2 = 1$. En déduire que toute forme quadratique non dégénérée sur un espace vectoriel de dimension strictement supérieure à 2 sur K admet un vecteur isotrope non nul.

3) Montrer que l'espace vectoriel K^n est somme directe Q-orthogonale de m plans hyperboliques et d'une droite non isotrope. En considérant le discriminant de Q, montrer que cette droite est engendrée par un vecteur x tel que $Q(x) = (-1)^m$.

4) En déduire que la forme quadratique Q sur l'espace vectoriel K^n est isomorphe á la forme quadratique $\underline{Q}$ sur l'espace vectoriel $K^m \oplus K^m \oplus K$ définie par

$$\underline{Q}(x, y, z) = 2(x_1y_1 + \ldots + x_my_m) + (-1)^m z^2$$

où $x, y \in K^m$ et $z \in K$ et que $N(p, n)$ est le nombre de solutions dans $K^m \oplus K^m \oplus K$ de l'équation $\underline{Q}(x, y, z) = 1$.

5) Pour $x \in K^m$, soit $N(x)$ le nombre de solutions $(y, z) \in K^m \oplus K$ de l'équation $\underline{Q}(x, y, z) = 1$. Montrer que si $x \neq 0$, alors $N(x) = p^m$.

Indication : pour tout $a \in K$, l'ensemble des $y \in K^m$ tels que $x_1y_1 + \ldots + x_my_m = a$ est un hyperplan affine dont on calculera le cardinal.

6) Calculer $N(x)$ lorsque $x = 0$.

Indication : remarquer que le nombre de $z \in K$ tels que $z^2 = (-1)^m$ est égal à 2 ou 0 selon que $(-1)^m$ est ou n'est pas un carré modulo p ; en déduire que

$$N(0) = ((-1)^{m\frac{p-1}{2}} + 1)p^m.$$

7) Déduire de 5) et 6) la formule :

$$N(p,n) = p^{n-1} + (-1)^{\frac{n-1}{2}\frac{p-1}{2}} p^{\frac{n-1}{2}}.$$

II. Calcul de $N(p,q)$ modulo q

On suppose désormais que $n = q$ est un nombre premier distinct de p et de 2. On va calculer $N(p,q)$ modulo q de deux façons différentes et en déduire la loi de réciprocité quadratique.

1) En utilisant le résultat de la première partie, montrer que

$$N(p,q) \equiv 1 + (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

modulo q.

2) On revient à la forme Q sur K^q. Soit $\lambda : K^q \to K^q$ tel que

$$\lambda(x_1, \ldots, x_q) = (x_2, \ldots, x_q, x_1).$$

Montrer que l'ensemble X des solutions de l'équation $Q(x) = 1$ est stable par λ. Montrer que la décomposition en cycles de λ, considérée comme une permutation de l'ensemble X, ne fait intervenir que des cycles de longueur q.

3) En déduire que le cardinal $N(p,q)$ de X est congru modulo q au cardinal F de l'ensemble des poins fixes de λ dans X.

Montrer que $F = 1 + \left(\frac{q}{p}\right)$.

Indication : remarquer que les points fixes de λ dans X sont les vecteurs de la forme $(x, \ldots, x)$ où $x \in K$ est tel que $qx^2 = 1$.

5) Déduire de ce qui précède la formule de réciprocité quadratique :

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$