UPS – Centre d'Orsay **Arithmétique – Maîtrise**
Mathématiques Année 2003–2004

FEUILLE D'EXERCICES n° 3

Exercice 1 –

a) On considère l'ensemble E des fonctions de $\mathbb{N}_{>0}$ dans $\mathbb{C}$, muni de la loi interne

$$f * g := n \to \sum_{ab=n} f(a)g(b).$$

On note $\mathbf{1}$ la fonction constante égale à 1 et ε la fonction définie par $\varepsilon(n) = 1$ si $n = 1$ et 0 sinon. f et g désignent des éléments de E.

i) Montrer que $*$ est abélienne, associative de neutre ε et que f est inversible si et seulement si $f(1) \neq 0$.

ii) On note μ l'inverse de $\mathbf{1}$. Montrer que $\mu(n) = (-1)^k$ si $n = p_1 \dots p_k$, où les p_i sont des premiers distincts, et 0 sinon.

iii) Montrer que si $f = \mathbf{1} * g$, alors $g = \mu * f$.

b) Soit $a_q(d)$ le nombre de polynômes unitaires, irréductibles, de degré $d \geqslant 1$ dans $\mathbb{F}_q$.

i) Montrer que la fonction a vérifie

$$\sum_{d|n} d a_q(d) = q^n.$$

[*faire une partition de* $\mathbb{F}_{q^n}$ *en regroupant les éléments de même polynôme minimal sur* $\mathbb{F}_q$. *Ou bien utiliser la décomposition en facteurs irréductibles de* $X^{q^n} - X$]

ii) En déduire une expression de $a_q(d)$; montrer qu'elle est strictement positive.

Exercice 2 – Soit $\mathbb{F}_q$ une extension finie de $\mathbb{F}_p$. Montrer les équivalences

a) $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$ si et seulement si il existe $\beta \in \mathbb{F}_q$, $\alpha = \beta - \beta^p$.

b) $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 1$ si et seulement si il existe $\beta \in \mathbb{F}_q$, $\alpha = \beta/\beta^p$.

Exercice 3 – On veut vérifier que pour tout $m > 0$ et tout corps fini $\mathbb{F}_q$, il existe un polynôme homogène de degré m dans $\mathbb{F}_q[X_1, \dots, X_m]$ sans 0 non triviaux. Soit $\omega_1, \dots, \omega_m$ une $\mathbb{F}_q$-base de $\mathbb{F}_q^m$; montrer que

$$f(X_1, \dots, X_m) := \prod_{i=1}^{m} \left(\omega_1^{q^i} X_1 + \cdots + \omega_m^{q^i} X_m\right)$$

répond à la question.

Exercice 4 – Calculer la fonction zêta associée sur $\mathbb{F}_q$

i) à la courbe affine $XY = 0$ et à sa complétion projective.

ii) même question avec la courbe $X^2 = Y^3$.

Exercice 5 – Montrer que la fonction zêta d'une courbe $\mathcal{C}$ est une fraction rationnelle si et seulement si il existe des nombres complexes α_i et β_j en nombre fini, tels que

$$\#\mathcal{C}(\mathbb{F}_{p^s}) = \sum_j \beta_j^s - \sum_i \alpha_i^s.$$

[*pour le sens difficile, écrire* $Z(T) = \prod(1-\alpha_i T)/\prod(1-\beta_j T)$ *et prendre la dérivée logarithmique.*]

Exercice 6 – Calculer la fonction zêta de la courbe affine $Y^2 = X^3 + X^2$, ainsi que celle de la courbe projective associée.

★ **Exercice 7** – Calculer la fonction zêta de la courbe projective $X^3 + Y^3 + Z^3 = 0$ sur $\mathbb{F}_4$, puis sur $\mathbb{F}_2$. [*Réponse :* $P_q(T)/(1-T)(1-qT)$, *avec* $P_2(T) = (1+2T^2)$, $P_4(T) = (1+2T)^2$]

★ **Exercice 8** – Soit p un premier impair et ψ le caractère additif donné par $\psi(x) = \exp(2i\pi x/p)$. On veut montrer que pour tout $c \in \mathbb{F}_p$, on a

$$(1) \qquad \sum_{\substack{a,b\in\mathbb{F}_p\\ ab=c}} \psi(a+b) = -\sum_{\substack{x\in\mathbb{F}_{p^2}\\ \mathrm{N}(x)=c}} \psi(\mathrm{Tr}(x)),$$

où N et Tr désignent respectivement la norme et la trace de $\mathbb{F}_{p^2}$ dans $\mathbb{F}_p$.

a) Vérifier (1) pour $c = 0$.

b) Si $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ est un caractère multiplicatif, et $f : \mathbb{F}_p^* \to \mathbb{C}$ un fonction quelconque, on appelle transformée de Mellin de f la fonction $\hat{f}(\chi) = \sum_{c\in\mathbb{F}_p^*} \chi(c) f(c)$. Montrer que

$$f(x) = \frac{1}{p-1}\sum_\chi \hat{f}(\chi)\overline{\chi(x)}, \quad \forall x \in \mathbb{F}_p^*,$$

où χ parcourt les caractères multiplicatifs de $\mathbb{F}_p^*$.

c) Montrer que les deux membres de (1) ont même transformées de Mellin [*les exprimer en termes de sommes de Gauss et utiliser Davenport-Hasse*]. Conclure.

d) Soit λ le caractère de Legendre modulo p. Montrer directement que

$$\#\{a, b \in \mathbb{F}_p \colon a + b = y, ab = c\} = \lambda(y^2 - 4c) - 1$$

$$\#\{x \in \mathbb{F}_{p^2} \colon \mathrm{Tr}(x) = y, \mathrm{N}(x) = c\} = 1 - \lambda(y^2 - 4c)$$

En déduire une autre démonstration de (1).

Exercice 9 – Soit k un corps de caractéristique différente de 2. On appelle conique une courbe $\mathcal{C}$ de degré 2, donnée par une forme quadratique en 3 variables à coefficients dans k, non dégénérée. On appelle *ouvert* de $\mathcal{C}$ le complémentaire d'une courbe (*i.e.* on rajoute une équation homogène du type $P(X, Y, Z) \neq 0$).

a) On s'intéresse au cercle $\mathcal{C} : X^2 + Y^2 = Z^2$.

i) On se restreint à l'ouvert $Z \neq 0$, i.e. à l'équation affine $X^2 + Y^2 = 1$. Ecrire $X + 1 = tY$ et en déduire une paramétrisation du cercle, à un nombre fini de points près, borné indépendamment de k. Interprétation géométrique ?

ii) Etendre la paramétrisation en une bijection de $\mathbb{P}^1(K)$ sur $\mathcal{C}(K)$, pour tout extension K de k, donnée par des polynômes homogènes sur chacun des ouverts $X + Z \neq 0$ et $X - Z \neq 0$ (par exemple). Que se passe-t-il sur leur intersection ?

b) $\mathcal{C}$ est maintenant une conique plane quelconque. Si $\mathcal{C}(k)$ est non vide, à un changement de repère linéaire près (défini sur k), on peut supposer que le point $(0 : 0 : 1)$ appartient à $\mathcal{C}(k)$: l'équation de $\mathcal{C}$ devient $ZF_1(X, Y) + F_2(X, Y) = 0$ où F_i est homogène de degré i.

i) Poser $tY = uX$ et construire une bijection de $\mathbb{P}^1(K)$ sur $\mathcal{C}(K)$.

ii) Montrer que sur des ouverts convenables, elle est donnée par des polynômes homogènes.

c) On suppose dorénavant que k est fini.

i) Montrer que $\mathcal{C}(k)$ est non vide.

ii) Calculer la fonction zêta de $\mathcal{C}$ sur k.