Université Paris Diderot
M1 Arithmétique
2009-2010

Feuille d'exercices II

Exercice 1 Soit G un groupe commutatif fini dont l'élément unité est noté comme e.

1) Montrer que, si G est cyclique, alors pour tout eniter $m > 0$, l'équation $x^m = e$ admet au plus m solutions dans G.

2) Soit g un élément du plus grand ordre dans G. Soit n son ordre. Montrer que, pour tout élément h de G, l'ordre de h divise n.

3) En déduire que, pour tout $h \in G$, on a $h^n = e$.

4) Montrer que la réciproque de 1) est aussi vraie.

Exercice 2 Soit R un anneau intègre.

1) Montrer que tout polynôme P de degré $d \geq 1$ dans $R[X]$ admet au plus d racines dans R. [*Indication : passer au corps des fractions de* R.]

2) En appliquant le résultat de 1) au cas où $P(X) = X^d - 1$, montrer que tout sous-groupe fini de $R^\times$ est cyclique.

3) En déduire que, si F est un corps fini, alors $F^\times$ est un groupe cyclique. Quel est l'ordre de ce groupe ?

Exercice 3 Soit p un nombre premier impaire. On désigne par f l'application de $(\mathbb{Z}/p\mathbb{Z})^\times$ vers lui-même qui envoie x en x^2. Soit Q_p l'image de l'application f.

1) Montrer que, si h est un générateur du groupe cyclique $(\mathbb{Z}/p\mathbb{Z})^\times$, alors Q_p coïncide avec l'ensemble des puissances paires de h.

2) En déduire le cardinale de Q_p.

3) Montrer que l'application $x \mapsto x^{(p-1)/2}$ est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^\times$ vers lui-même dont le noyau est Q_p. Déterminer son image.

4) Montrer que la classe de -1 est dans Q_p si et seulement si $p \equiv 1 \pmod 4$.

5) En déduire qu'il y a une infinité de nombres premiers de la forme $4m+1$. [*Indication : on peut considérer le nombre* $(2p_1 \cdots p_r)^2+1$, *où* $p_1, \ldots, p_r$ *sont les premiers* r *nombres premiers de la forme* $4m+1$.]

Exercice 4 Soit $m \geq 2$ un entier. On appelle *caractère de Dirichlet* modulo m toute fonction arithmétique χ (i.e. fonction de $\mathbb{N}_*$ vers $\mathbb{C}$) tel qu'il existe un morphisme de groupe $\bar{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ avec

$$\chi(n) = \begin{cases} 0, & \mathrm{pgcd}(n,m) > 1, \\ \bar{\chi}(\bar{n}), & \mathrm{pgcd}(n,m) = 1, \end{cases}$$

où $\bar{n}$ désigne la classe de n dans $\mathbb{Z}/m\mathbb{Z}$.

1) Montrer que tout caractère de Dirichlet est une fonction arithmétique complètement multiplicative (autrement dit, $\chi(nd) = \chi(n)\chi(d)$ pour tout $(n,d) \in \mathbb{N}_*^2$).

2) Soit p un nombre premier. Montrer que le symbole de Legendre modulo p est un caractère de Dirichlet.

Exercice 5 Soit p un nombre premier impair.

1) Soit g un générateur du groupe $\mathbb{F}_{p^2}^{\times}$.

   On note $h = g^{(p^2-1)/8}$. Déterminer l'ordre de h dans $\mathbb{F}_{p^2}^{\times}$.

2) Soient $\tau = h + h^{-1}$ et $\mathbf{1}$ l'élément unité de $\mathbb{F}_{p^2}^{\times}$. Montrer les relations suivantes :

$$\tau^2 = \mathbf{1}+\mathbf{1}, \quad \tau^p = \left(\frac{2}{p}\right)\tau = h^p+h^{-p}.$$

3) En déduire que

$$\tau^p = \begin{cases} \tau, & \text{si } p \equiv \pm 1 \pmod 8, \\ -\tau, & \text{si } p \equiv \pm 3 \pmod 8 \end{cases}$$

4) En déduire que

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

5) En déduire qu'il y a une infinité de nombres premiers de la forme $8m+7$.[*Indication : on peut considérer le nombre* $(4p_1 \cdots p_r)^2 - 2$, *où* $p_1, \ldots, p_r$ *sont les premiers* r *nombres premiers de la forme* $8m+7$.]

Exercice 6 Soient p et q deux nombres premiers impairs, $p \neq q$. Le but de cet exercice est de redémontrer la loi de réciprocité quadratique par la théorie des corps finis. Dans cet exercice, on fixe un générateur g du groupe $\mathbb{F}_{q^{p-1}}^{\times}$.

1) Montrer que q^{p-1} est congru à 1 modulo p.

2) Soit $h = g^{(q^{p-1}-1)/p}$. Pour tout $a \in \mathbb{Z}$, soit $\tau_a := \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) h^{am}$. Montrer que $\tau_a = \left(\frac{a}{p}\right)\tau_1$.

3) Montrer que $\tau_1^2 = (-1)^{(p-1)/2} p\,\mathbf{1}$, où $\mathbf{1}$ est l'élément unité dans $\mathbb{F}_{q^{p-1}}$. En déduire que $\tau_1 \in \mathbb{F}_q$ si et seulement si $(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) = 1$.

4) Soit x un élément de $\mathbb{F}_{q^{p-1}}$. Montrer que $x \in \mathbb{F}_q$ si et seulement si $x^q = x$.

5) Montrer que $\tau_1^q = \tau_q$. Conclure.

Exercice 7 Rappelons la loi de réciprocité quadratique pour le symbole de Jacobi :

$$\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}, \quad \left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}, \quad \left(\frac{a}{b}\right)$$

où a et b sont des entiers impaires premiers entre eux.

1) Soit $p > 3$ un nombre premier. Montrer que 3 est un résidu quadratique

modulo p si et seulement si $p \equiv \pm 1 \pmod{12}$.

2) Calculer $\left(\frac{113}{997}\right)$.

Exercice 8 Soit p un nombre premier impair. On rappelle qu'un caractère de $\mathbb{F}_p^\times$ est par définition un morphisme de groupes de $\mathbb{F}_p^\times$ vers $\mathbb{C}^\times$. En particulier, l'application de $\varepsilon : \mathbb{F}_p^\times \to \mathbb{C}^\times$ qui prend identiquement la valeur 1 est un caractère de $\mathbb{F}_p^\times$, appelé le caractère principal. Il est utile dans cet exercice d'étendre le domaine de définition d'un caractère (de $\mathbb{F}_p^\times$) à $\mathbb{F}_p$ en prenant

$$\chi(0) := \begin{cases} 0, & \chi \neq \varepsilon, \\ 1, & \chi = \varepsilon. \end{cases}$$

Si $(\chi_1, \ldots, \chi_n)$ est une famille de ca-

ractères de $\mathbb{F}_p^\times$, la somme de Jacobi de $(\chi_1, \ldots, \chi_n)$ est définie comme

$$J(\chi_1, \ldots, \chi_n) := \sum_{\substack{(t_1,\ldots,t_n)\in\mathbb{F}_p^n \\ t_1+\cdots+t_n=1}} \chi_1(t_1)\cdots\chi_n(t_n).$$

On note en outre

$$J_0(\chi_1, \ldots, \chi_n) := \sum_{\substack{(t_1,\ldots,t_n)\in\mathbb{F}_p^n \\ t_1+\cdots+t_n=0}} \chi_1(t_1)\cdots\chi_n(t_n).$$

1) Soit χ un caractère de $\mathbb{F}_p^\times$. Montrer que

$$\sum_{t\in\mathbb{F}_p} \chi(t) = \begin{cases} 0, & \chi \neq \varepsilon, \\ p, & \chi = \varepsilon. \end{cases}$$

2) Soit G l'ensemble des caractères de $\mathbb{F}_p^\times$. Montrer que G est un groupe cyclique d'ordre $p-1$.

3) Montrer que le symbole de Legendre λ est le seul caractère d'ordre 2 de $\mathbb{F}_p^\times$.

4) Soient a un élement de $\mathbb{F}_p$ et n un diviseur de $p-1$.

   (i) On suppose que l'équation $x^n = a$ n'ait pas de solution dans $\mathbb{F}_p$. Montrer qu'il existe un caractère $\chi \in G$ d'ordre n tel que $\chi(a) \neq 1$ ([*Indication : on peut considérer* $\eta^{(p-1)/n}$, *où* η *est un générateur de* G.]).

   (ii) On désigne par $N(x^n = a)$ le nombre des solutions de l'équation $x^n = a$ dans $\mathbb{F}_p$. Montrer que, si $a \in \mathbb{F}_p^\times$, alors $N(x^n = a)$ est ou bien nul, ou bien égal à n. [*Indication : étudier l'équation*

$x^n = 1.]$

(iii) Montrer que

$$N(x^n = a) = \sum_{\chi \in G,\, \chi^n = \varepsilon} \chi(a).$$

(iv) En déduire que

$$N(x^2 = a) = 1 + \left(\frac{a}{p}\right).$$

(v) Montrer que

$$N(x^2 + y^2 = 1) = p + 2\sum_{a} \left(\frac{a}{p}\right) + \sum_{a+b=1} \left(\frac{a}{p}\right) \Big($$

où $N(x^2 + y^2 = 1)$ désigne le nombre des solution de l'équation $x^2 + y^2 = 1$ dans $\mathbb{F}_p^2$.

5) Déterminer les valeurs de $J_0(\varepsilon, \ldots, \varepsilon)$ et de $J(\varepsilon, \ldots, \varepsilon)$.

6) On suppose que $\chi_1 \neq \varepsilon$ et $\chi_n = \varepsilon$.

Montrer que

$$J_0(\chi_1, \ldots, \chi_n) = J(\chi_1, \ldots, \chi_n) = 0.$$

7) On suppose que $\chi_1 \cdots \chi_n \neq \varepsilon$, montrer que

$$J_0(\chi_1, \ldots, \chi_n) = 0.$$

8) On suppose que les $\chi_1, \ldots, \chi_n$ soient non-principaux, et que leur produit $\chi_1 \cdots \chi_n$ soit non-principal non plus. Montrer que

$$J(\chi_1, \ldots, \chi_n) g(\chi_1 \cdots \chi_n) = g(\chi_1) \cdots g(\chi_n),$$

où g est la somme de Gauss :

$$g(\chi) := \sum_{t \in \mathbb{F}_p} \chi(t) e^{2\pi i t/p}.$$

9) Pour $a \in \mathbb{F}_p$ et $\chi \in G$, on note $g_a(\chi) := \sum_{t \in \mathbb{F}_p} \chi(t) e^{2\pi i a t/p}$. En calculant $\sum_a g_a(\chi) g_a(\overline{\chi})$ par deux

méthodes, montrer que $|g(\chi)| = \sqrt{p}$ lorsque $\chi \neq \varepsilon$.

10) En déduire que, si $\chi \neq \varepsilon$, alors $g(\chi)g(\overline{\chi}) = \chi(-1)p$.

11) On suppose que les $\chi_1, \ldots, \chi_n$ soient non-principaux, et que $\chi_1 \cdots \chi_n = \varepsilon$. Montrer que

$$g(\chi_1) \cdots g(\chi_n) = \chi_n(-1)pJ(\chi_1, \ldots, \chi_{n-1}).$$

12) On désigne par $N(x_1^2 + \cdots + x_n^2 = 1)$ le nombre des solutions de l'équation $x_1^2 + \cdots + x_n^2 = 1$ dans $\mathbb{F}_p^n$. Montrer que

$$N(x_1^2 + \cdots + x_n^2 = 1) = p^{n-1} + J(\underbrace{\lambda, \ldots, \lambda}_{n \text{ copies}}),$$

où λ est le symbole de Legendre.

13) Déterminer la valeur de $N(x_1^2 + \cdots + x_n^2 = 1)$, on discutera la parité de n.