ENS Cachan
M1 mathématiques Arithmétique - 2014-2015

Exercices - Feuille 1

I. Corps finis

1. Soit $K = \mathbb{F}_{p^r}$ un corps fini. Montrer que pour tout élément $\beta \in K$, il existe un unique élément $\alpha \in K$ tel que $\alpha^p = \beta$.
2. Dans cet exercice, on va étudier le corps $\mathbb{F}_{16}$ explicitement.
   1. Montrer que $f = X^4 + X + 1 \in \mathbb{F}_2[X]$ est un polynôme irréductible. En déduire que $K = \mathbb{F}_2[X]/(f)$ est une extension de degré 4 de $\mathbb{F}_2$. K^* est alors un groupe abélien de ordre 15, vérifier que la classe de X dans K, notée par α, est un générateur du groupe K^*. Donner une base de K vu comme un espace vectoriel sur $\mathbb{F}_2$. Exprimer α^8 comme une combinaison linéaire de cette base.
   2. Soit ϕ un automorphisme (de corps) de K. Vérifier que $\phi_{|\mathbb{F}_2} = \mathrm{id}_{\mathbb{F}_2}$, que ϕ est une bijection $\mathbb{F}_2$-linéaire, et que ϕ induit un automorphisme du groupe K^*. Montrer que ϕ est déterminé par l'image de α et que ϕ est de la forme $x \mapsto x^s$ avec s un certain entier strictement positif.
   3. Montrer que $\phi(\alpha) \in K$ est une racine de f. En déduire que $\alpha, \alpha^2, \alpha^4, \alpha^8$ sont les quatre racines distinctes de f.
   4. Montrer que $g = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$ est aussi irréductible. Noter par β la classe de X dans $L = \mathbb{F}_2[X]/(g)$, montrer que $\beta^{-1} \in L$ est une racine de f. Expliciter un isomorphisme ψ de $K = \mathbb{F}_2(\alpha)$ vers L. Décrire tout isomorphisme $K \to L$ à l'aide de ψ et du Frobenius Fr de K.
   5. Montrer que $h = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$ est aussi irréductible. Noter par γ la classe de X dans $M = \mathbb{F}_2[X]/(h)$. Est-ce que γ est un générateur du groupe cyclique M^* ? Calculer l'ordre de $\gamma \in M^*$. Montrer que $\gamma \mapsto \alpha^3$ induit un morphisme de corps $M \to K$, montrer que c'est un isomorphisme.
   6. Trouver tous les polynômes irréductibles unitaires de degré 4 dans $\mathbb{F}_2[X]$. En déduire que tout corps fini ayant 16 éléments est isomorphe à K.

3. Soit $a \in \mathbb{F}_p$. En comptant $\{x^2 | x \in \mathbb{F}_p\}$ et $\{a - y^2 | y \in \mathbb{F}_p\}$, montrer que on peut toujours écrire a comme une somme de deux carrés dans $\mathbb{F}_p$.
4. Le but de cet exercice est de montrer le théorème de Erdös–Ginzburg–Ziv : Soit p un nombre premier. Étant donnés $2p-1$ entiers $a_1, \ldots, a_{2p-1}$, il existe toujours p entiers d'entre eux tels que leur somme soit divisible par p.
   1. Considérons les polynômes $f, g \in \mathbb{F}_p[X_1, \ldots, X_{2p-1}]$ définis par
   $$f = X_1^{p-1} + \cdots + X_{2p-1}^{p-1} \text{ et } g = a_1 X_1^{p-1} + \cdots + a_{2p-1} X_{2p-1}^{p-1}.$$
   Montrer que $f(x) \equiv g(x) \equiv 0 \pmod p$ a toujours des solutions $x = (x_1, \ldots, x_{2p-1})$ non nulles $(\mathrm{mod}\ p)$.
   2. Montrer la relation $f(x) \equiv Card(I_x) \pmod p$ où $I_x = \{i | x_i \neq 0 \pmod p\}$.
   3. Montrer la relation $g(x) \equiv \sum_{i \in I_x} a_i \pmod p$.
   4. En déduire le théorème.

II. "Chinese remainder theorem"

1. Soient $m_1, \ldots, m_r$ des entiers positifs deux à deux premiers. Montrer qu'il existe un nombre entier e_1 tel que $e_1 \equiv 1 \pmod{m_1}$ et $e_1 \equiv 0 \pmod{m_j} \forall j \neq 1$. En déduire que pour tout entier x_i, il existe un entier x tel que $x \equiv x_i \pmod{m_i}$ pour tout i.
2. m_i comme ci-dessus, $f \in \mathbb{Z}[X]$. Montrer que $f(X) \equiv 0 \pmod{m_1 \ldots m_r}$ a une solution dans $\mathbb{Z}$ si et seulement si $f(X) \equiv 0 \pmod{m_i}$ a une solution dans $\mathbb{Z}$ pour tout i.

III. Réciprocité quadratique

Soit p un nombre premier, montrer les énoncés suivants.

1. 5 est un carré modulo p si et seulement si $p = 5$ ou $p \equiv \pm 1 \pmod{5}$.
2. 3 est un carré modulo p si et seulement si $p = 3$ ou $p \equiv \pm 1 \pmod{12}$.
3. 7 est un carré modulo p si et seulement si $p = 7$ ou $p \equiv \pm 1, \pm 3, \pm 9 \pmod{28}$.

IV. Nombres p-adiques

Soit $f \in \mathbb{Z}[X]$ le polynôme $f = (X^2 - 13)(X^2 - 17)(X^2 - 13 \cdot 17)$.

1. Pour $p \neq 2, 13, 17$, montrer que $f(X) = 0$ a une solution modulo p, en déduire que $f(X) = 0$ a une solution dans $\mathbb{Z}_p$.
2. Montrer que $f(X) = 0$ a une solution dans $\mathbb{Z}_2$, $\mathbb{Z}_{13}$ et $\mathbb{Z}_{17}$.
3. Conclure que l'équation $f(X) = 0$ ne vérifie pas le principe local-global de Hasse.