Exercices - Feuille I `À rendre pour le 5 Mai 2004`

Exercice I1. Soient p un nombre premier, $A \in \mathbf{F}_p[X]$ un polynôme `unitaire` non nul et $m \geq 1$ un entier positif. Montrer que les deux conditions suivantes sont équivalentes.
(i) A est `produit de polynômes unitaires irréductibles sur` $\mathbf{F}_p$ `deux à deux distincts` de degré m.
(ii) $A(X)$ divise $X^{p^m} - X$ et pour tout diviseur premier ℓ de m,

$$\mathrm{pgcd}(X^{p^{m/\ell}} - X, A(X)) = 1.$$

Exercice I2. Soient p un nombre premier, $A \in \mathbf{F}_p[X]$ un polynôme unitaire sans facteurs carrés, et $A = A_1 \cdots A_r$ sa décomposition en facteurs irréductibles unitaires sur $\mathbf{F}_p$.

a) Soit $Q \in \mathbf{F}_p[X]$ un polynôme de degré $< \deg A$.
Montrer que les deux conditions suivantes sont équivalentes:
(i) Pour tout $i = 1, \ldots, r$, il existe $\alpha_i \in \mathbf{F}_p$ tel que

$$Q \equiv \alpha_i \pmod{A_i}$$

(ii) $Q(X)^p \equiv Q(X) \pmod{A}$.

b) Montrer qu'il y a exactement p^r polynômes $Q \in \mathbf{F}_p[X]$ de degré $< \deg A$ vérifiant les conditions équivalentes de la question a), et expliciter une bijection entre ces polynômes et les éléments de $\mathbf{F}_p^r$.

c) On désigne par R l'anneau quotient $\mathbf{F}_p[X]/A(X)\mathbf{F}_p[X]$, par $S : R \to R$ l'endomorphisme $Q \mapsto Q^p$ du $\mathbf{F}_p$-espace vectoriel R et on pose $N = \ker(S - I)$. Quelle est la dimension du $\mathbf{F}_p$-espace vectoriel N?

d) On suppose $r \geq 2$. Soit $Q \in N$ de degré ≥ 1. Vérifier

$$A = \prod_{\alpha \in \mathbf{F}_p} \mathrm{pgcd}(A, Q - \alpha).$$

Montrer qu'il existe $\alpha \in \mathbf{F}_p$ tel que $\mathrm{pgcd}(A, Q - \alpha)$ soit différent de 1 et de A.

Exercice I3. Soient n un entier ≥ 2. Soit s le nombre d'entiers b dans l'intervalle $1 \leq b < n$, qui sont premiers avec n et tels que

$$b^{n-1} \not\equiv 1 \pmod{n}.$$

a) Montrer que l'on a soit $s = 0$, soit $s \geq \varphi(n)/2$.

b) On suppose $s = 0$ (autrement dit n est soit un nombre premier, soit un *nombre de Carmichael*). Montrer que n est sans facteur carré.

`Indication.` *Écrire $n = p^r m$ avec p premier, $r \geq 2$ et m non divisible par p. Soit g un générateur du groupe cyclique $(\mathbf{Z}/p^2\mathbf{Z})^\times$. Montrer qu'il existe un entier b premier avec m et congru à g modulo p^2.*

Exercice I4. Soit n un entier > 1. Soient u et v deux entiers positifs tels que $n - 1 = uv$. On suppose que pour tout premier q divisant u, si q^{r_q} désigne la plus grande puissance de q qui divise u, il existe un entier positif a_q tel que

$$a_q^{q^{r_q}} \equiv 1 \pmod{n}$$

et

$$\operatorname{pgcd}\left(a_q^{q^{r_q-1}} - 1, n\right) = 1.$$

Montrer que tous les diviseurs de n sont congrus à 1 modulo u.

En déduire que si, de plus, $u \geq v - 1$, alors n est premier.

`Indication.` *On peut commencer par le cas où u est de la forme q^r avec q premier et $r \geq 1$. Dans ce cas particulier on pourra considérer l'ordre de a modulo p.*