Université Paris Diderot
M1 Arithmétique
2010-2011

Feuille d'exercices VIII

Exercice 1 Soit p un nombre premier. On désigne par $|\cdot|_p$ la valeur absolue p-adique de $\mathbb{Q}$, normalisée de sorte que $|p|_p = p^{-1}$. Soit $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ par rapport à la valeur absolue $|\cdot|_p$ et par $\mathbb{Z}_p$ le sous-anneau de $\mathbb{Q}_p$ des éléments a tels que $|a|_p \leqslant 1$. On dit qu'un polynôme $F(X) = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}_p[X]$ est *primitif* si

$$\max\{|a_0|, \ldots, |a_n|\} = 1.$$

Le but de cet exercice est de montrer le lemme de Hensel : *Si $F \in \mathbb{Z}_p[X]$ est un polynôme prmitif dont la réduction modulo p se décompose en produit de deux polynômes g et h dans $\mathbb{F}_p[X]$ qui sont premiers entre eux, alors il existe deux polynômes G et H dans $\mathbb{Z}_p[X]$ dont les réductions modulo p sont respectivement g et h, et tels que $F = GH$ et $\deg(G) = \deg(g)$.*

Dans la suite, on fixe F, g et h comme dans l'énoncé du lemme de Hensel. Soient en outre $d = \deg(F)$ et $m = \deg(g)$.

1) Montrer qu'un polynôme $P \in \mathbb{Z}_p[X]$ est primitif si et seulement si sa réduction modulo p est non-nulle.
2) Montrer que $d - m \geqslant \deg(h)$.
3) Choisissons deux polynômes G_0 et H_0 dans $\mathbb{Z}_p[X]$ dont les réductions modulo p sont respectivement g et h, et tels que $\deg(G_0) = \deg(g)$ et $\deg(H_0) = \deg(h)$. Montrer qu'il existe deux éléments A et B dans $\mathbb{Z}_p[X]$ tels que $AG_0 + BH_0 - 1 \in p\mathbb{Z}_p[X]$.
4) Montrer que le coefficient dominant de G_0 est un élément inversible dans $\mathbb{Z}_p$.

Dans la suite, on suppose que $F \neq G_0H_0$ (car sinon il n'y a rien à démontrer). On choisit, parmi les coefficients des polynômes $F - G_0H_0$ et $AG_0 + BH_0 - 1$, un élément non-nul ϑ dont la valeur absolue est maximale.

5) Montrer que $|\vartheta|_p < 1$.

On construit par récurrence deux suites de polynômes

$$G_n = G_0 + \vartheta P_1 + \cdots + \vartheta^n P_n,$$
$$H_n = H_0 + \vartheta Q_1 + \cdots + \vartheta^n Q_n,$$

où P_i et Q_i $(i = 1, \ldots, n)$ sont des polynômes dans $\mathbb{Z}_p[X]$ de degrés $< m$ et $\leqslant d - m$ respectivement, telles que la condition $(\mathbb{P}_n)$: $F - G_nH_n \in \vartheta^{n+1}\mathbb{Z}_p[X]$ soit satisfaite.

6) Montrer que la condition (P_0) est satisfaite avec le choix de G_0, H_0 et ϑ comme ci-dessus.

Supposons que l'on a construit $P_1, \ldots, P_{n-1}, Q_1, \ldots, Q_{n-1}$ de sorte que les conditions $(\mathbb{P}_0), \ldots, (\mathbb{P}_{n-1})$ soient satisfaites.

7) Montrer que, si P_n et Q_n sont des polynômes qui permettent de construire G_n et H_n de telle sorte que la condition $(\mathbb{P}_n)$ soit vérifiée, alors on a

$$F_n - G_{n-1}Q_n - H_{n-1}P_n \in \vartheta\mathbb{Z}_p[X], \qquad (*)$$

où $F_n := \vartheta^{-n}(F - G_{n-1}H_{n-1})$.

8) Montrer que la relation $(*)$ est satisfaite si on prend $Q_n = AF_n$ et $P_n = BF_n$. Ce choix est-il convenable pour construire G_n et H_n ?

9) Montrer qu'il existe un unique polynôme $P_n \in \mathbb{Z}_p[X]$ de degré $< m$ tel que $BF_n - P_n$ soit divisible (dans $\mathbb{Z}_p[X]$) par G_0.

10) Soit $R_n \in \mathbb{Z}_p[X]$ le polynôme tel que $BF_n - P_n = R_n G_0$. Moontrer que

$$G_0(AF_n + H_n R_n) + H_0 P_n - F_n \in \vartheta \mathbb{Z}_p[X].$$

11) Soit Q_n le polynôme obtenu de $AF_n + H_n R_n$ en gardant les termes de coefficients de valeur absolue 1 et éliminant les autres. Montrer que $G_0 Q_n - H_0 P_n - F_n \in \vartheta \mathbb{Z}_p[X]$ et $\deg(Q_n) \leqslant d - m$.

12) En déduire que les polynômes G_n et H_n construits à partir de P_n et Q_n comme dans les questions 9) et 11) vérifient la condition $(\mathbb{P}_n)$.

13) Conclure.

14) Application : montre que toute racine $p^{\text{ième}}$ de l'unité est contenue dans $\mathbb{Z}_p$.

Exercice 2 Pour tout entier $n \geqslant 1$, soit Φ_n le $n^{\text{ième}}$ polynôme cyclotomique. Montrer que

$$\Phi_n(X) = \prod_{d|n} (X^{n/d} - 1)^{\mu(d)},$$

où μ est la fonction de Möbius.