TP 9 : Lemme de Hensel et factorisation sur $\mathbf{Z}[X]$

► **Prérequis** : *Chapitre 7 du poly.*

1 Hensel

Soient p un nombre premier, deux entiers $m \geqslant k \geqslant 1$, un entier x et un polynôme $P \in \mathbf{Z}[X]$ tels que $P(x) \equiv 0 \pmod{p}$ et $P'(x) \not\equiv 0 \pmod{p}$.

1. Cette question est fausse comme on le constate avec $p = 3$, $P = X - 4$ et $k = m = 2$. En effet, $x = 1$ est solution modulo 3 mais la seule solution modulo 3^4 est 4 qui n'est pas congrue à 1 modulo 9.
2. Écrire une fonction prenant en arguments p, P, x et $m \geqslant k$ qui vérifie que $P(x) \equiv 0 \pmod{p^k}$ et que des conditions adéquates sont réunies puis qui retourne un élément $y \in \mathbf{Z}/p^n\mathbf{Z}$ tel que $P(y) \equiv 0 \pmod{p^n}$ et $x \equiv y \pmod{p^k}$.
3. Déterminer les racines carrées de 2 dand $\mathbf{Z}/7^{35}\mathbf{Z}$.

2 Racines de l'unité

1. À quelle condition sur un nombre premier p le polynôme $X^n - 1$ est-il séparable sur $\mathbf{Z}/p\mathbf{Z}$?
2. Soient p premier et n entier tels que p ne divise pas n. Montrer que le polynôme $X^n - 1 \in \mathbf{F}_p[X]$ est scindé si et seulement si n divise $p - 1$.
3. Déterminer les racines 4-ièmes de l'unité dans $\mathbf{Z}/13^{12}\mathbf{Z}$.

3 Factorisation dans $\mathbf{Z}[X]$

3.1 Un premier exemple

On considère $P = X^4 + X^3 - X + 1 \in \mathbf{Z}[X]$. Le but de cette section est de montrer, avec les moyens du cours, que P est irréductible dans $\mathbf{Z}[X]$.

1. Montrer que si P n'est pas irréductible alors il existe $Q \in \mathbf{Z}[X]$ unitaire de degré ≤ 2 divisant P et tel que $||Q||_\infty \leqslant 8$.
2. Déterminer les diviseurs unitaires de la classe de P dans $\mathbf{F}_{17}[X]$.
3. Conclure que P est irréductible dans $\mathbf{Q}[X]$ et dans $\mathbf{Z}[X]$.

3.2 Le cas général

L'objectif de cette section est de proposer un algorithme plus général.

1. Soit $P \in \mathbb{Z}[X]$. Implémenter une fonction qui prend en entrées un entier n, deux polynômes G et H ainsi qu'un nombre premier p tels que $\mathrm{Res}(G, H) \not\equiv 0 \pmod{p}$ et $F \equiv GH \pmod{p}$ avec H unitaire et vérifiant $\deg(G) + \deg(H) = \deg(P)$ ainsi que deux polynômes U et V vérifiant $UG + VH \equiv 1 \pmod{p}$ avec $\deg(U) < \deg(H)$ et $\deg(V) < \deg(G)$ et qui renvoie $\tilde{G}, \tilde{H}, \tilde{U}, \tilde{V}$ congrus à G, H, U, V modulo p et vérifiant

$$P \equiv \tilde{G}\tilde{H} \left(\mathrm{mod}\ p^{2^n}\right) \quad \text{et} \quad \tilde{U}\tilde{G} + \tilde{V}\tilde{H} \equiv 1 \left(\mathrm{mod}\ p^{2^n}\right)$$

avec $\deg(\tilde{G}) + \deg(\tilde{H}) = \deg(P)$ et $\deg(\tilde{U}) < \deg(\tilde{H})$ et $\deg(\tilde{V}) < \deg(\tilde{G})$.

2. Décrire une procédure qui permet de se ramener, pour factoriser un polynôme de $\mathbf{Q}[X]$, à factoriser un polynôme unitaire de $\mathbf{Z}[X]$ sans facteur carré.

3. Écrire une fonction qui choisit un nombre premier p ne divisant pas le discriminant de P.

4. Écrire une fonction qui calcule un entier d tel qu'il suffit de remonter la factorisation de P modulo p modulo p^d.

5. Écrire une fonction qui fournit la liste des parties $I \subseteq \{1, \ldots, k\}$ de cardinal compris entre 1 et $k-1$ ainsi qu'une fonction qui à une telle partition et à une factorisation de $P = Q_1 \cdots Q_k$ modulo p^d renvoie un représentant Q_I de

$$\prod_{i \in I} Q_i$$

dans $\mathbf{Z}[X]$ tel que $||Q_I||_\infty \leqslant \lfloor \frac{p^d}{2} \rfloor$.

6. Implémenter un algorithme de factorisation d'un polynôme de $\mathbf{Q}[X]$. Tester votre algorithme.

7. Que pouvez-vous dire en termes de complexité de l'algorithme proposé ?