RETOUR TP 9 – LEMME DE HENSEL ET FACTORISATION SUR $\mathbb{Z}[X]$

1 Hensel

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

2. Cette question est fautive comme on le constate avec $p = 3$, $P = X^3 - 4$ et $k = m = 2$. En effet, $x = 1$ est solution modulo 3 mais la seule solution modulo 3^2 est 4 qui n'est pas congrue à 1 modulo 9.

2 Racines de l'unité

1. Il est clair que $X^n - 1$ est séparable sur $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si, $\text{pgcd}(p, n) = 1$. Il est en effet clair que cette condition est nécessaire pour garantir que $\text{pgcd}(nX^{n-1}, X^n - 1)$ soit égal à 1 et elle est aussi suffisante.
2. On a vu et établi dans un TP précédent que chaque polynôme cyclotomique Φ_d avec $d \mid n$ (dont le produit vaut $X^n - 1$) sont des produits de facteurs irréductibles tous de même degré égal à l'ordre de p modulo d . Ainsi, chaque facteur de $X^n - 1$ est scindé si, et seulement si, l'ordre de p modulo d est égal à 1 pour tout d divisant n . Autrement dit, on veut que $p \equiv 1 \pmod{d}$ pour tout diviseur de n , ce qui équivaut bien au fait que n divise $p - 1$.
3. On est dans le cas d'application du lemme précédent et il suffit donc de factoriser $X^4 - 1$ qui est scindé modulo p avant d'appliquer Hensel.

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

3.1 Un premier exemple

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

1. Si P n'est pas irréductible alors admet un diviseur unitaire de degré 1 ou un diviseur de degré 2. Par le Corollaire 7.9, un tel diviseur Q vérifie

$$\|Q\|_\infty \leq 2^2 \|P\|_2.$$

Sage fournit $\|P\|_2 = 2$ et on a bien le résultat.

2. On utilise Sage (on pourrait le faire avec Berlekamp ou en énumérant la liste des diviseurs irréductibles de degré 2 et 3).
3. Si P n'est pas irréductible dans $\mathbb{Q}[X]$, il admet un facteur de norme infinie inférieure à 8 qui se réduit donc modulo 17. Un des facteurs de P modulo 17 doit donc provenir de ce facteur sur $\mathbb{Q}$ de norme infinie inférieure à 8. Or, si c'est $X^2 + 4X + 7$, alors $X^2 + 4X + 7$ doit diviser P (noter qu'on a pas le choix pour les coefficients qui sont ici modulo 17 pour que ce polynôme provienne d'un polynôme dont tous les coefficients sont plus petits que 8 car ajouter ou enlever un multiple de 17 les fait dépasser 8 en valeurs absolue). Or, une division euclidienne révèle que ce n'est pas le cas. Dans ce cas, le second facteur doit provenir du facteur de degré 2 et de norme infinie inférieure à 8 et ce dernier ne peut qu'être la réduction de $X^2 - 3X + 5$ qui ne divise pas non plus P et par conséquent par conséquent P est irréductible sur $\mathbb{Q}[X]$. On conclut à l'irréductibilité sur $\mathbb{Z}[X]$ car de contenu égal à 1.

3.2 Le cas général

L'objectif de cette section est de proposer un algorithme plus général. Cette section est en bonus et ne sera pas corrigée mais je vous encourage à la chercher, si vous avez des questions sur le sujet, vous pouvez m'écrire par mail!

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 $\text{Res}(G, H) \not\equiv 0 \pmod{p}$ 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

$$P \equiv \tilde{G}\tilde{H} \pmod{p^{2^n}} \quad \text{et} \quad \tilde{U}\tilde{G} + \tilde{V}\tilde{H} \equiv 1 \pmod{p^{2^n}}$$

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 $\mathbb{Q}[X]$, à factoriser un polynôme unitaire de $\mathbb{Z}[X]$ 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 $I \subseteq \{1, \dots, k\}$ 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 $\|Q_I\|_\infty \leq \lfloor \frac{p^d}{2} \rfloor$.

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 ?