Université de Bordeaux
Mathématiques

Préparation à l'agrégation
2015–2016

Lemme de Hensel

Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury demande que la discussion soit accompagnée d'exemples traités sur ordinateur. Il est souhaitable que vous organisiez votre présentation comme si le jury n'avait pas connaissance du texte. Le jury aura néanmoins le texte sous les yeux pendant votre exposé.

1. Cas régulier

Le texte est consacré à l'étude du résultat suivant, appelé « Lemme de Hensel » :

Lemme 1.1. *Soit P un polynôme de $\mathbb{Z}[X]$ et p un nombre premier. Soit n un entier supérieur ou égal à 1. On suppose que l'on dispose d'un entier x tel que*

$$P(x) \equiv 0 \pmod{p^n} \quad et \quad P'(x) \not\equiv 0 \pmod{p}.$$

Alors il existe un entier y dans $\mathbb{Z}$ tel que

$$y \equiv x \pmod{p^n} \quad et \quad P(y) \equiv 0 \pmod{p^{2n}}.$$

De plus, cet entier est unique modulo p^{2n}. On peut le prendre égal à $x - P(x)s$, où s est tel que $sP'(x) \equiv 1 \pmod{p^n}$.

Remarque 1.2. On reconnaît ici une version algébrique de la méthode de Newton, qui s'écrirait $y = x - P(x)P'(x)^{-1}$.

Preuve. On cherche l'entier y sous la forme $x + tp^n$; ce sera un antécédent "bien choisi" de x par la surjection canonique $\mathbb{Z}/p^{2n}\mathbb{Z} \twoheadrightarrow \mathbb{Z}/p^n\mathbb{Z}$. On écrit la formule de Taylor à l'ordre 1

$$P(x + tp^n) = P(x) + tp^n P'(x) + t^2 p^{2n} R(x),$$

où $R \in \mathbb{Z}[X]$. Ainsi,

$$P(x + tp^n) \equiv P(x) + tp^n P'(x) \pmod{p^{2n}}.$$

Posons $P(x) = p^n P_0$, où $P_0 \in \mathbb{Z}$. Alors $P(x + tp^n) \equiv 0 \pmod{p^{2n}}$ si et seulement si

$$t \equiv -P'(x)^{-1} P_0 \pmod{p^n},$$

où $P'(x)^{-1}$ est l'inverse de $P'(x)$ modulo p^n, qui existe d'après les hypothèses. □

Remarque 1.3. On doit ici calculer à chaque étape un inverse modulaire. On peut pour cela utiliser directement l'algorithme d'Euclide étendu. On peut également utiliser le résultat suivant :

Lemme 1.4.**.** *Si v est un inverse de u modulo N, alors $2v - uv^2$ est un inverse de u modulo N^2.*

Preuve. On peut le voir directement, en calculant $1 - u(2v - uv^2) = (uv - 1)^2$; on peut aussi remarquer que c'est une conséquence du lemme de Hensel, pour le polynôme $P(x) = ux - 1$. □

Corollaire 1.5. *Si p est un nombre premier impair et si a est un entier premier à p qui est reste quadratique modulo p, alors a est reste quadratique modulo p^n pour tout $n \geqslant 1$.*

Preuve. On considère le polynôme $P(X) = X^2 - a$. L'équation à résoudre est donc

$$P(x) \equiv 0 \pmod{p^n}.$$

Soit x un entier tel que $P(x) \equiv 0 \bmod p$. Alors $P'(x) = 2x$ est premier à p. On peut alors utiliser le théorème précédent pour montrer par récurrence l'existence d'une solution. □

2. Cas singulier

On ne suppose plus que $P'(x) \not\equiv 0 \pmod{p}$. Le théorème ci-dessus peut être adapté dans ce cadre plus général. Pour $x \in \mathbb{Z}$, $x \neq 0$, on appelle valuation de x en p, notée $v_p(x)$, l'unique entier v tel que $p^v \mid x$, mais $p^{v+1} \nmid x$.

Théorème 2.1. *Soit $P \in \mathbb{Z}[X]$ et p un nombre premier. Soit x un entier, tel que $P'(x) \neq 0$ et soit $v = v_p(P'(x))$. Soit $n \geqslant 2v + 1$ un entier. Si $y \equiv x \bmod p^{n-v}$, alors $v_p(P'(y)) = v$ et $P(x) \equiv P(y) \pmod{p^n}$.*

Si de plus $P(x) \equiv 0 \pmod{p^n}$, alors il existe un entier y dans $\mathbb{Z}$ tel que

$$y \equiv x \pmod{p^{n-v}} \quad \text{et} \quad P(y) \equiv 0 \pmod{p^{2(n-v)}}.$$

De plus, cet entier est unique modulo p^{2n-3v}. On peut le prendre égal à

$$x - \frac{P(x)}{p^v} s,$$

où s est tel que $sP'(x)/p^v \equiv 1 \pmod{p^{n-2v}}$.

Preuve. La démonstration est analogue. Posons $y = x + tp^{n-v}$; la formule de Taylor donne maintenant

$$P(x + tp^{n-v}) \equiv P(x) + tp^{n-v}P'(x) \pmod{p^{2(n-v)}}, \tag{1}$$

$$P'(x + tp^{n-v}) \equiv P'(x) + tp^{n-v}P''(x) \pmod{p^{2(n-v)}}, \tag{2}$$

soit $P(y) \equiv P(x) \pmod{p^n}$ et $P'(y) \equiv P'(x) \pmod{p^{n-v}}$. Comme $n \geqslant 2v + 1$, on en déduit que $P'(y) \equiv P'(x) \pmod{p^{v+1}}$, soit $v_p(P'(y)) = v$.

Enfin, si $P(x) \equiv 0 \pmod{p^n}$, on déduit de (1) que

$$P(y) \equiv 0 \pmod{p^{2(n-v)}}$$

si et seulement si

$$t\frac{P'(x)}{p^v} \equiv -\frac{P(x)}{p^n} \pmod{p^{n-2v}},$$

qui adment une unique solution t modulo p^{n-2v}. □

Corollaire 2.2. *Soit a est un entier impair. Alors a est reste quadratique modulo 2^n pour tout entier $n \geqslant 3$ si et seulement si $a \equiv 1 \pmod 8$.*

Preuve. L'entier a est un carré modulo 8 si et seulement si $a \equiv 1 \bmod 8$. On applique le théorème précédent au polynôme $P(X) = X^2 - a$. □

3. Racine carrée dans $\mathbb{Z}/n\mathbb{Z}$

Si n est une puissance d'un nombre premier, il reste à considérer le cas où l'on rechercherait une racine carrée d'un entier a divisible par p.

Proposition 3.1. *Soient p un nombre premier, α, β deux entiers tels que $0 \leqslant \alpha < \beta$, et a un entier premier à p. Alors ap^α est reste quadratique modulo p^β si et seulement si α est pair et a est reste quadratique modulo $p^{\beta-\alpha}$.*

Si n n'est pas une puissance d'un nombre premier, on se ramène à ce cas en utilisant le théorème chinois.