Nombres p-adiques et Factorisation de polynômes

Problème I (Lemme de Hensel)

On rappelle le principe de l'itération de Newton (méthodes des tangentes). Si f est sympathique et x_0 pas trop mal choisi, la suite définie par

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

converge vers une solution de l'équation $f(x) = 0$. On en étudie ici une version arithmétique. Soit, donc, f un polynome à coefficients entiers et p un nombre premier. On dit que $a \in \mathbb{Z}$ est *singulier* si $f'(a) \equiv 0 \pmod p$, et non singulier sinon.

1) On suppose que a est non singulier et que $f(a) \equiv 0 \pmod{p^i}$, $i > 0$.

a) montrer qu'il existe $c = c(i)$, unique modulo p et donné par une formule simple, tel que $f(a + cp^i) \equiv 0 \pmod{p^{i+1}}$ [*penser à la formule de Taylor*].

b) En déduire que si a est une racine de f modulo p (non singulière), l'équation $f(x) = 0 \pmod{p^i}$ a une solution a_i pour tout i. On peut même choisir un système (a_i) de solutions "compatibles", telles que $a_i \equiv a_j \pmod{p^i}$ si $i \leqslant j$.

2) On suppose maintenant que a est singulier, et toujours $f(a) \equiv 0 \pmod{p^i}$, $i > 0$. Montrer que si $b \equiv a \pmod{p^i}$, alors $f(b) \equiv f(a) \pmod{p^{i+1}}$.

★ **3)** [*généralisation*] Si $a \in \mathbb{Z} - \{0\}$, il existe un unique n tel que $a = p^n u$, avec $(p, u) = 1$. On l'appelle *valuation p-adique* de a, et on note $v_p(a) := n$. On pose $v_p(0) := +\infty$.

Soit $a \in \mathbb{Z}$ tel que $f(a) \equiv 0 \pmod{p^{n+k}}$ et $v_p(f'(a)) = k$. On suppose $k < n$. Montrer qu'il existe $b \in \mathbb{Z}$, $b \equiv a \pmod{p^n}$, unique modulo p^{n+1}, tel que $f(b) \equiv 0 \pmod{p^{n+k+1}}$ et $v_p(f'(b)) = k$.

Moralité : grâce à l'itération de Newton, une bonne approximation initiale a d'une racine de f [*telle que* $v_p(f(a)) > 2v_p(f'(a))$] peut se relever modulo une puissance de p arbitraire. Les résultats sont plus parlants si on pose $|x|_p := p^{-v_p(x)}$ pour $x \in \mathbb{Q}$: il s'agit bien d'une valeur absolue, et on peut munir $\mathbb{Q}$ de la topologie associée. Dans ce cas $b \equiv a \pmod{p^n}$ se lit $|b - a|_p \leqslant p^{-n}$: a et b sont proches. Ainsi, un système (a_i) de solutions compatibles est une suite de Cauchy.

4) On peut représenter la situation en tracant des lignes horizontales L_i correspondant à la situation modulo p^i ; sur chaque L_i on marque un point par racine modulo p^i. Puis, si $a \in L_i$, $b \in L_{i+1}$ sont deux racines avec $a \equiv b \pmod{p^i}$ ("b est au-dessus de a" ou "relève a"), on trace un trait entre a et b. On obtient ainsi un arbre représentant les solutions [*faire les dessins sur papier...*]

On vient des voir des critères permettant d'affirmer que cet arbre a des branches infinies. Expérimenter avec les cas suivants (on donnera le nombre de branches infinies et les valuations intéressantes) :

a) $f = x^3 + x + 1$, $p = 31$.
b) $f = x^2 + 1$, $p = 2, 3, 5$ ou 7.
c) $f = x^5 + 8x + 16$, $p = 2$.

★ **5)** Faire un programme général dont les données sont le polynome f, le nombre premier p, et un niveau n. En sortie on demande les solutions modulo p^i pour tout $i \leqslant n$, et l'arbre correspondant [*pour évaluer un polynome modulo m, utiliser la forme neutre* `Eval(f, x = a) mod m` *plutôt que* `subs(f, x = a) mod m`] (pourquoi ?)

6) Calculer l'arbre des solutions de $x^4 - 10x^3 + 35x^2 - 50x + 24 = 0$ modulo 3^n. Que dire des racines de ce polynôme dans $\mathbb{Z}$?

★ **7)** On suppose maintenant que f est unitaire. Étant donnés $B, C \in \mathbb{Z}[X]$ unitaires, tels que $(\overline{B}, \overline{C}) = 1$ dans $\mathbb{F}_p[X]$, et $f \equiv BC \pmod{p^n}$, $n \geqslant 1$, construire B' et $C' \in \mathbb{Z}[X]$ unitaires qui relèvent B et C modulo p^{n+1}, c'est-à-dire tels que $A = B'C' \pmod{p^{n+1}}$ et $B' \equiv B \pmod{p^n}$, $C' \equiv C \pmod{p^n}$. Montrer que B' et C' sont uniques modulo p^{n+1}.

Problème II (Nombres p-adiques)

On introduit $\mathbb{Z}_p$, l'ensemble des "branches infinies" ou "systèmes compatibles" modulo p. Plus précisément, c'est l'ensemble des suites (a_i), où a_i est dans $\mathbb{Z}/p^i\mathbb{Z}$, vérifiant $a_i \equiv a_j \pmod{p^i}$ quand $i \leqslant j$. On le munit de l'addition et de la multiplication composante par composante. Pour tout $k > 0$, on a des réductions naturelles de $\mathbb{Z}_p$ dans $\mathbb{Z}/p^k\mathbb{Z}$: $(a_i) \mapsto a_k$. C'est un anneau qui contient $\mathbb{Z}$ [$a \mapsto (a \pmod{p^i})$ *est injective*], il est donc de caractéristique 0.

En particulier, chaque branche infinie de $f(x) = 0$ modulo p^* est une solution de l'équation dans $\mathbb{Z}_p$. Comme $\mathbb{Z}_p$ est sans diviseurs de 0 [*à voir*], il y a au plus autant de solutions que le degré de f.

1) Montrer que tout rationnel a/b de dénominateur premier à p appartient à $\mathbb{Z}_p$ [*contempler* $f(x) = bx - a$]. Montrer que $1/p \notin \mathbb{Z}_p$, c'est-à-dire qu'il n'existe pas $x \in \mathbb{Z}_p$ tel que $px = 1$.

Note : Pour pallier à ce dernier problème on introduit $\mathbb{Q}_p$ le corps des fractions de $\mathbb{Z}_p$, qui contient $\mathbb{Q}$ puisque $\mathbb{Z} \subset \mathbb{Z}_p$. Tout élément de $\mathbb{Q}_p^*$ s'écrit façon unique sous la forme $p^n u$ avec $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p$, $u \not\equiv 0 \pmod{p}$. On montre qu'un tel u est inversible dans $\mathbb{Z}_p$. On pose $v_p(p^n u) := n$, et la définition coïncide avec celle du premier problème quand $x \in \mathbb{Q}$. On pose $|x|_p = p^{-v_p(x)}$, c'est une norme sur $\mathbb{Q}_p$, qui est *complet* pour la topologie correspondante. En fait, on aurait pu le construire comme ca, c'est le complété de $\mathbb{Q}$ pour la valeur absolue p-adique : le "plus petit" corps contenant $\mathbb{Q}$ tel que toute suite de Cauchy (pour $|\ |_p$!) converge. De même qu'on peut définir $\mathbb{R}$ comme le complété de $\mathbb{Q}$ pour la valeur absolue usuelle. Toutes ces constructions sont dues à Hensel (vers 1900).

On peut faire de l'analyse (convergence, intégration, ...) sur $\mathbb{Q}_p$ comme on le fait sur $\mathbb{R}$; on définit aussi $\mathbb{C}_p$ où tous les polynômes se scindent, des fonctions $\mathbb{C}_p$-analytiques, ... Et extraire de tout celà de l'information arithmétique ("modulo p^k", bien sur).

2) On se donne à nouveau f, une racine non singulière a de f modulo p, et la suite $c(i)$ fournie par le lemme de Hensel. Montrer que, dans la notation du **I**, on a $a_n = \sum_{i=0}^{n} c(i)p^i$. Interpréter.

3) Si $a > 0$ et $b > 1$ sont deux entiers, $(b, pa) = 1$, on écrit

$$a/b = \sum_{i=0}^{n} c(i)p^i + \frac{\lambda}{b}p^{n+1}, \quad \lambda \in \mathbb{Z}$$

comme ci-dessus, grâce au lemme de Hensel. Calculer les $c(i)$ pour $a/b = 5/3$ et $p < 30$. Que remarque-t-on ?

a) On définit (c_i) et (v_i) par les relations de récurrence

$$\begin{cases} v_0 &= a \\ v_i &= bc_i + pv_{i+1}, \quad i \geqslant 0, \text{ où } 0 \leqslant c_i < p, \text{ et } v_i \in \mathbb{Z} \end{cases}$$

Montrer que ces entiers sont bien déterminés. Expérimenter comme ci-dessus. Conjecture ?

★ b) En déduire que $0 > v_n > -b$ pour n assez grand, puis que les $c(i)$ sont ultimement périodiques, de période l'ordre de p dans $(\mathbb{Z}/b\mathbb{Z})^*$ [*trouver une formule simple pour* $v_i \pmod{b}$]

Problème III (Factorisation sur un corps fini (Berlekamp, 1968))

Pour simplifier, on se limite au cas d'un corps premier. Soit $C \in \mathbb{F}_p[X]$, *sans facteurs carrés* ; on veut déterminer une factorisation en produit d'irréductibles distincts $C = \prod_{i=1}^{r} P_i$. D'après le lemme chinois, l'algèbre $A = \mathbb{F}_p[X]/(C)$ est isomorphe au produit $\prod \mathbb{F}_p[X]/(P_i)$. Comme les

P_i sont irréductibles et $\mathbb{F}_p[X]$ principal, chaque $\mathbb{F}_p[X]/(P_i)$ est un corps (à $p^{\deg(P_i)}$ éléments). L'application de Frobenius $\Phi_p : A \to A$, donnée par $X \mapsto X^p$ est un morphisme d'algèbre.

1) Montrer que $\Phi_p(v) = v$ si et seulement si $v \equiv \alpha_i \pmod{P_i}$ pour tout i, où $\alpha_i \in \mathbb{F}_p$.

2) En déduire que le noyau K de $\Phi_p - \mathrm{Id}$ est de dimension r.

3) Pour $1 \leqslant i \leqslant r$, on note $\pi_i : \mathbb{F}_p[X]/(C) \to \mathbb{F}_p[X]/(P_i)$ la projection canonique ; par définition, $\pi_i(K) = \mathbb{F}_p$. Soit $(v_1, \dots, v_r)$ une base de K. Montrer que si $i \neq j$, alors il existe $1 \leqslant k \leqslant r$ tel que $\pi_i(v_k) \neq \pi_j(v_k)$ [*cette identité a lieu dans* $\mathbb{F}_p$].

4) En déduire que si on connait k et $\alpha := \pi_i(v_k) \in \mathbb{F}_p$ comme ci-dessus, alors $\mathrm{pgcd}(v_k - \alpha, C)$ fournit un diviseur non trivial de C.

★ **5)** En déduire que l'algorithme suivant factorise C :

```
on pose i := 1 ; L := [C] ;        # liste de polynomes dont le produit est C
tant que longueur(L) < r
  on prend Q := L[i] ;
  pour tout k ⩽ r, α ∈ F_p
    on pose D := pgcd(v_k − α, Q) ;
    si 0 < degré(D) < degré(Q),
      remplacer Q par D dans L et rajouter Q/D a la fin
      recommencer au début de la boucle extérieure
  poser i := i+1 ;    # Q est irréductible, on n'y touche plus
renvoyer L
```

[*Essentiellement, comme on ne connaît ni k ni* α*, on essaie les rp combinaisons possibles.*]

★★ **6)** Comment se ramener au cas sans facteur carrés à partir d'un polynôme C quelconque. [C *est sans facteur carré ssi* $\mathrm{pgcd}(C, C') = 1$.] Evaluer la complexité totale de l'algorithme.

★ **7)** On suppose $p > 2$. Plutôt que de chercher α au hasard dans $\mathbb{F}_p$ (p possibilités), on va utiliser le fait que $\alpha^{(p-1)/2} \in \{-1, 0, 1\}$. Si $v \in K$, et $u := v^{(p-1)/2}$ que dire des $\pi_i(u)$, puis de $\mathrm{pgcd}(C, u - 1)$? En déduire une amélioration probabiliste de la méthode ci-dessus. Montrer qu'un $v \in K$ choisi uniformément au hasard permet de factoriser C avec probabilité $\geqslant 4/9$ [*commencer par une formule exacte en fonction de p et r*].

Problème IV (Factorisation sur $\mathbb{Z}$ (Zassenhaus, 1969))

Soit A un polynôme à coefficients entiers que l'on désire factoriser dans $\mathbb{Q}[X]$. On donne d'abord une idée générale de l'algorithme : les preuves des assertions successives sont reportés aux questions.

On peut supposer que A est unitaire, dans $\mathbb{Z}[X]$, sans facteurs carrés. Si B est un facteur de A, on a $\|B\|_\infty \leqslant K$ pour une borne explicite K ne dépendant que de A. On choisit $p > 2K$ tel que $A \pmod p$ soit sans facteur carré, on factorise A sur $\mathbb{F}_p$:

$$A \equiv \prod_{i=1}^{r} P_i \pmod{p},$$

où les P_i sont irréductibles, unitaires et distincts. Alors chaque facteur sur $\mathbb{Z}$ est de la forme $\prod_{i \in I} P_i$ modulo p pour un unique $I \subset \{1, \dots, r\}$, et il ne reste plus qu'à essayer les 2^r parties I possibles, en relevant les coefficients des polynômes correspondant de $\mathbb{F}_p$ à $]-p/2, p/2[$.

1) Soit $A \in \mathbb{Q}[X]$, que l'on désire factoriser. Expliquer comment se ramener au cas ou A est unitaire, dans $\mathbb{Z}[X]$, sans facteur carré.

2) Montrer que si B et $C \in \mathbb{Z}[X]$ sont premiers entre eux, il existe U, V dans $\mathbb{Z}[X]$ et un entier $n \neq 0$ tels que $BU + CV = n$ [$\mathbb{Z}[X]$ *n'est pas euclidien, mais* $\mathbb{Q}[X]$ *si*]. En déduire qu'à un nombre fini de premiers près (lesquels ?), B et C sont aussi premiers entre eux dans $\mathbb{F}_p[X]$. En pratique, comment choisir p tel que $A \pmod p$ n'ait pas de facteurs carrés dans $\mathbb{F}_p[X]$?

3) On fixe $I \subset \{1, \dots, r\}$. Montrer qu'il existe au plus un $B \in \mathbb{Z}[X]$ tel que $B \equiv \prod_{i \in I} P_i \pmod p$ et $\|B\|_\infty \leqslant K$. En déduire un algorithme fini permettant de déterminer tous les facteurs irréductibles de A dans $\mathbb{Q}[X]$.

★★ **4)** [*Hensel généralisé*] Soit ℓ un nombre premier et $A \equiv \prod_{i=1}^r P_i$ la factorisation en irréductibles unitaires distincts de $\mathbb{F}_\ell[X]$. Montrer que cette factorisation se relève modulo p^n, et que les P_i permettent d'obtenir une factorisation de A en produit d'irréductibles dans $\mathbb{Z}_\ell[X]$.

5) Dans la question IV.3, on n'utilise pas le fait que p soit premier, à part pour factoriser A modulo p. Adapter l'algorithme pour le choix $p = \ell^k$, ℓ premier. On peut maintenant choisir ℓ petit et k minimal tel que $\ell^k > 2K$. Quel est l'intérêt de ce nouvel algorithme ?

Appendice : la borne de Landau-Mignotte

Théorème 1. *Si* $A = \sum_{i=0}^m a_i X^i \in \mathbb{C}[X]$ *et* $B = \sum_{i=0}^n b_i X^i$ *divise* A*, on a*

$$|b_i| \leqslant \binom{n-1}{i} ||A||_2 + \binom{n-1}{i-1} |a_m|, \text{ pour tout } 0 \leqslant i \leqslant n$$

1) Si $1 \leqslant x_1 \leqslant \cdots \leqslant x_m$ sont des réels, de produit M, alors la fonction symétrique élémentaire $\sigma_{m,k} = \sum x_{i_1} \dots x_{i_k}$ vérifie trivialement $\sigma_{m,k} \leqslant \binom{m}{k} M$. Montrer qu'en fait

$$\sigma_{m,k} \leqslant \binom{m-1}{k-1} M + \binom{m-1}{k},$$

le maximum étant atteint ssi $x_1 = \cdots = x_{m-1} = 1$. [*Remplacer* (x_1, x_m) *par* $(1, x_1 x_m)$ *augmente* $\sigma_{m,k}$ *de* $\sigma_{m-2,k-1}(x_m - 1)(x_1 - 1) > 0$.]

2) Soit

$$A = \sum_{i=0}^m a_i X^i = a_m \prod_{i=0}^m (X - \alpha_i) \in \mathbb{C}[X].$$

On note

$$M(A) := |a_m| \prod_{i:\ |\alpha_i| > 1} |\alpha_i| \quad \text{et} \quad m(A) := |a_m| \prod_{i:\ |\alpha_i| < 1} |\alpha_i|,$$

($M(A)$ est la *mesure de Mahler de* A.) Appliquer la question précédente aux $x_i := \max(1, |\alpha_i|)$ et montrer que

$$|a_{m-i}| \leqslant \binom{m-1}{i-1} M(A) + \binom{m-1}{i} |a_m|$$

3) Montrer que $||(X - \alpha)A(X)||_2 = ||(\overline{\alpha}X - 1)A(X)||_2$. En déduire que, si

$$C(X) := a_m \prod_{i:\ |\alpha_i| \geqslant 1} (X - \alpha_i) \prod_{i:\ |\alpha_i| < 1} (\overline{\alpha_i} X - 1)$$

on a $||A||_2^2 = ||C||_2^2 \geqslant M(A)^2 + m(A)^2$, soit finalement $M(A) < ||A||_2$. Conclure.