COMPOSITION DE MATHEMATIQUES

Epreuve commune aux ENS de Cachan et de Lyon

Durée : 4 heures

Introduction

Le but du problème est l'étude d'une technique intervenant dans un domaine lié à l'arithmétique, domaine appelé "théorie des nombres p-adiques". Une vague idée que l'on peut donner de l'adjectif p-adique est celle d'une suite d'entiers $(x_i)_{i\geq 1}$ vérifiant la condition de *cohérence* :

$$x_{i+1} \equiv x_i \pmod{p^i} \quad \text{pour tout } i.$$

$$\begin{array}{cc} & \vdots \\ x_3 : & \mathbf{Z}/p^3\mathbf{Z} \\ & \downarrow \\ x_2 : & \mathbf{Z}/p^2\mathbf{Z} \\ & \downarrow \\ x_1 : & \mathbf{Z}/p\mathbf{Z} \end{array}$$

Un cas fréquent est celui où p est un nombre premier, mais ce n'est pas là le seul exemple. On peut évoquer une telle suite à l'aide d'un schéma (c.f. la figure encadrée à droite) dans lequel les flèches verticales désignent successivement les réductions modulo p, modulo p^2 ...

L'épreuve est essentiellement consacrée au développement d'une méthode permettant (sous certaines conditions) de "remonter" une solution x d'une congruence polynomiale $P(x) \equiv 0 \pmod p$ en une solution de la même congruence mais modulo p^2 puis p^3, etc. Le problème fournit ensuite quelques applications de cette méthode à des polynômes ou à des matrices (et non pas à des nombres !) avec comme conséquences :

- surjectivité de l'exponentielle : $\mathrm{M}_n(\mathbf{C}) \to \mathrm{GL}_n(\mathbf{C})$
- existence de racines carrées, cubiques, ..., dans $\mathrm{GL}_n(\mathbf{C})$
- existence de la décomposition $A = D+N$, D diagonalisable, N nilpotente, $DN = ND$

Partie I : Préliminaires relatifs aux congruences et aux polynômes

Soit $\mathbf{A}$ un anneau *commutatif* unitaire dont l'élément unité est noté 1. On rappelle que la relation $x \equiv y \pmod a$, pour $x, y, a, \in \mathbf{A}$ signifie que $x - y \in \mathbf{A}a = \{\lambda a \mid \lambda \in \mathbf{A}\}$; on rappelle également qu'un élément $z \in \mathbf{A}$ est *inversible modulo a* s'il existe un $z' \in \mathbf{A}$ tel que $zz' \equiv 1 \pmod a$; on dit alors que l'élément $z' \in \mathbf{A}$ est *un* inverse de z modulo a.

1. Vérifier *rapidement* que :

$$x \equiv y \pmod a,\ x' \equiv y' \pmod a \ \Rightarrow\ x + x' \equiv y + y' \pmod a \text{ et } xx' \equiv yy' \pmod a.$$

et que $x \equiv y \pmod a \Rightarrow P(x) \equiv P(y) \pmod a$ pour tout polynôme P à coefficients dans $\mathbf{A}$.

2. Vérifier qu'un élément $z \in \mathbf{A}$ inversible modulo a et inversible modulo b est inversible modulo ab ; en particulier si z est inversible modulo a, il est inversible modulo a^i pour tout $i \in \mathbb{N}^*$.

On note $\mathbf{A}[X]$ l'anneau des polynômes à coefficients dans $\mathbf{A}$: $\mathbf{A}[X]$ est donc constitué des sommes $a_0 + a_1 X + \cdots + a_n X^n$, où les a_i appartiennent à $\mathbf{A}$; les opérations (addition, multiplication) sont définies de manière habituelle et confèrent à $\mathbf{A}[X]$ une structure d'anneau commutatif unitaire. La dérivée de $P(X) = a_0 + a_1 X + a_2 X^2 \cdots + a_n X^n$, notée $P'(X)$, est le polynôme $a_1 + 2a_2 X + \cdots + n a_n X^{n-1}$. On désigne par $\mathbf{A}[X,Y]$ l'anneau $\mathbf{A}[X][Y]$.

3. Soit $P \in \mathbf{A}[X]$. En utilisant l'identité $X^n - Y^n = (X-Y)(X^{n-1} + X^{n-2}Y + \cdots + XY^{n-2} + Y^{n-1})$, montrer l'existence d'un polynôme $Q(X,Y) \in \mathbf{A}[X,Y]$ tel que $P(Y) - P(X) = (Y-X)Q(X,Y)$.
Que vaut $Q(X,X)$? Montrer également l'existence d'un polynôme $R(X,Y) \in \mathbf{A}[X,Y]$ tel que :

$$P(X+Y) = P(X) + YP'(X) + Y^2 R(X,Y).$$

Quelle relation existe-t-il entre Q et R ?

Partie II : Une méthode de "remontée modulaire"

Dans toute cette partie, on désigne par $\mathbf{A}$ un anneau *commutatif* unitaire, par P un polynôme à coefficients dans $\mathbf{A}$, et par a un élément de l'anneau $\mathbf{A}$.

1. Soit $x \in \mathbf{A}$ tel que $P(x) \equiv 0 \pmod{a^i}$ où i est un entier ≥ 1. Si $P'(x)$ est inversible modulo a, montrer l'existence d'un $\lambda \in \mathbf{A}$ pour lequel $y = x + \lambda a^i$ vérifie la congruence :

$$P(y) \equiv 0 \pmod{a^{i+1}}.$$

Montrer que la classe de y modulo a^{i+1} ne dépend pas du choix d'un inverse de $P'(x)$ modulo a ; expliciter y en fonction de x et d'*un* inverse de $P'(x)$ modulo a ;

2. Un exemple : soit z' un inverse modulo a d'un élément z. Comment appliquer la question précédente pour exhiber l'élément $z'(2 - zz')$ comme un inverse de z modulo a^2 ?

3. Soit une solution $x = x_1$ de $P(x) \equiv 0 \pmod{a}$ telle que $P'(x_1)$ soit inversible modulo a ; en utilisant la question **I.1**, expliquer comment construire par récurrence une suite $(x_i)_{i \geq 1}$ telle que :

$$P(x_i) \equiv 0 \pmod{a^i}, \qquad x_{i+1} \equiv x_i \pmod{a^i}.$$

Cette construction utilise *un* inverse de $P'(x_1)$ modulo a ; montrer que le choix d'un autre inverse conduit à une suite $(y_i)_{i \geq 1}$ telle que :

$$x_i \equiv y_i \pmod{a^i} \quad \text{pour tout } i.$$

4. Soit $i \geq 1$ fixé et $x, y \in \mathbf{A}$ vérifiant :

$$y \equiv x \pmod{a}, \quad P(y) \equiv P(x) \pmod{a^i}, \quad P'(x) \text{ inversible modulo } a.$$

En utilisant la question **I.3**, montrer que $y \equiv x \pmod{a^i}$.

5. On reprend les hypothèses et les notations de la question **II.3**. Montrer que pour $i \geq 1$ fixé, le système de congruences :

$$P(z) \equiv 0 \pmod{a^i}, \qquad z \equiv x_1 \pmod{a},$$

admet une unique solution z modulo a^i, égale à x_i.

Partie III : Troncature de l'exponentielle et du logarithme

Etant donné deux polynômes P, Q à coefficients dans $\mathbb{C}$, $Q \neq 0$, on note $P \bmod Q$ le reste de la division de P par Q : c'est l'unique polynôme R vérifiant :

$$\deg R < \deg Q, \qquad R \equiv P \pmod{Q} \qquad (\text{on convient que } \deg 0 = -\infty).$$

On définit une famille de polynômes "exponentielles tronquées" $(e_n)_{n \geq 1}$ à coefficients dans $\mathbb{Q}$ par :

$$e_1(T) = 1, \qquad e_2(T) = 1 + T, \qquad e_3(T) = 1 + T + \frac{T^2}{2}, \quad \ldots,$$

$$e_n(T) = 1 + \frac{T}{1!} + \frac{T^2}{2!} + \cdots + \frac{T^{n-1}}{(n-1)!}$$

1. En appliquant la partie **II** à l'anneau $\mathbf{A} = \mathbb{Q}[T]$, montrer l'existence et l'unicité d'un polynôme $l_n(T)$, de degré $< n$, à coefficients dans $\mathbb{Q}$, tel que :

$$(1) \qquad l_n(1) = 0, \qquad e_n(l_n(1+T)) \equiv 1 + T \pmod{T^n}$$

2. Pour $m \leq n$ calculer $e_m(l_n(1+T)) \bmod T^m$ puis $l_n(1+T) \bmod T^m$. En déduire, en dérivant la congruence (1) de la question précédente, le polynôme $l_n'(1+T)$ puis expliciter le polynôme $l_n(1+T)$.

3. On souhaite montrer que $l_n(e_n(T)) \equiv T \pmod{T^n}$; pour cela on pose $Q_n(T) = l_n(e_n(T))$. Calculer $e_n(Q_n(T)) \bmod T^n$ puis en déduire $Q_n(T) \bmod T^n$.

4. On rappelle qu'une matrice $A \in \mathrm{M}_n(\mathbb{C})$ est nilpotente si l'une de ses puissances est nulle et qu'une matrice unipotente est une matrice de la forme $\mathrm{I}_n + A$ où A est une matrice nilpotente (I_n désigne la matrice identité $n \times n$). Montrer que l'exponentielle réalise une bijection de l'ensemble des matrices nilpotentes de $\mathrm{M}_n(\mathbb{C})$ sur l'ensemble des matrices unipotentes de $\mathrm{M}_n(\mathbb{C})$; montrer que cette bijection et son inverse sont des applications polynomiales "à coefficients rationnels" que l'on explicitera.

5. Soit $\lambda \in \mathbb{C} - \{0\}$; si A est une matrice telle que $A - \lambda \mathrm{I}_n$ soit nilpotente, montrer l'existence de $B \in \mathrm{M}_n(\mathbb{C})$ telle que $\exp(B) = A$. En déduire que l'exponentielle réalise une surjection de $\mathrm{M}_n(\mathbb{C})$ sur $\mathrm{GL}_n(\mathbb{C})$. Est-ce une injection ?

Partie IV : Racines m-ièmes dans $\mathrm{GL}_n(\mathbb{R})$ ou $\mathrm{GL}_n(\mathbb{C})$

On applique la partie **II** à l'anneau $\mathbf{A} = K[X]$ où K désigne un sous-corps de $\mathbb{C}$ et on fournit quelques applications à l'anneau de matrices $\mathrm{M}_n(\mathbb{R})$ ou $\mathrm{M}_n(\mathbb{C})$.

1. Soit λ un élément *non nul* de K possédant une racine cubique dans K ; montrer que, quelque soit $k \in \mathbb{N}^*$, la congruence suivante :

$$Q(X)^3 \equiv X \pmod{(X - \lambda)^k},$$

admet une solution $Q(X) \in K[X]$.

2. Plus généralement, soient $\lambda \in K$ et $P \in K[X]$ tel que $P(x) = \lambda$ ait une solution $\mu \in K$ vérifiant $P'(\mu) \neq 0$; montrer que, quelque soit $k \in \mathbb{N}^*$, la congruence suivante :

$$P(Q(X)) \equiv X \pmod{(X - \lambda)^k},$$

admet une solution $Q(X) \in K[X]$.

3. Soient $T_1, T_2 \in K[X]$ deux polynômes *premiers entre eux* ; on suppose qu'il existe des polynômes $Q_1, Q_2 \in K[X]$ tels que :

$$P(Q_1(X)) \equiv X \pmod{T_1}, \qquad P(Q_2(X)) \equiv X \pmod{T_2}.$$

Montrer qu'il existe un polynôme $Q \in K[X]$ tel que $P(Q(X)) \equiv X \pmod{T_1 T_2}$.

4. On suppose que l'application $K \ni x \to P(x) \in K$ est surjective et que $T \in K[X]$ est un polynôme *scindé sur* K vérifiant :

$$\text{si } P(\mu) \text{ est racine de } T \text{ alors } P'(\mu) \neq 0.$$

Déduire des questions précédentes que l'équation suivante admet une solution en $Q(X) \in K[X]$:

$$P(Q(X)) \equiv X \pmod{T(X)}.$$

Examiner le cas particulier $P(X) = X^m$ pour $m \in \mathbb{N}^*$.

5. Soit $m \in \mathbb{N}^*$; en appliquant la question précédente, montrer que pour toute matrice inversible $A \in \mathrm{GL}_n(\mathbb{C})$ il existe $B \in \mathrm{GL}_n(\mathbb{C})$, *polynôme en* A, tel que $B^m = A$. Question analogue pour $\mathrm{GL}_n(\mathbb{R})$ en supposant que m impair et que $A \in \mathrm{GL}_n(\mathbb{R})$ a toutes ses valeurs propres réelles.

6. Soit $aX^2 + bX + c$ ($a \neq 0$) un trinôme à coefficients *réels* sans racine réelle. Caractériser, à l'aide d'une racine $\alpha \in \mathbb{C}\backslash\mathbb{R}$ de aX^2+bX+c, les polynômes *réels* multiples de aX^2+bX+c. Montrer que pour $m \in \mathbb{N}^*$, la congruence $Q(X)^m \equiv X \pmod{aX^2+bX+c}$ admet une solution $Q(X) \in \mathbb{R}[X]$ de degré 1.

En déduire que pour tout $m \in \mathbb{N}^*$ et $k \in \mathbb{N}^*$, la congruence :

$$Q(X)^m \equiv X \pmod{(aX^2+bX+c)^k},$$

admet une solution $Q(X) \in \mathbb{R}[X]$.

7. Plus généralement, soit $T(X) \in \mathbb{R}[X]$ sans racine réelle. Montrer que pour $m \in \mathbb{N}^*$, la congruence :

$$Q(X)^m \equiv X \pmod{T(X)},$$

admet une solution $Q(X) \in \mathbb{R}[X]$. En déduire que si $A \in \mathrm{M}_n(\mathbb{R})$ est sans valeur propre réelle, elle possède, pour tout $m \in \mathbb{N}^*$, une racine m-ième dans $\mathrm{M}_n(\mathbb{R})$ qui est un polynôme en A.

Partie V : A propos de la décomposition "diagonalisable + nilpotente"

On désigne dans cette partie par A une matrice $n \times n$ à coefficients dans un sous-corps K de $\mathbb{C}$ (par exemple l'un des trois corps $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) ; on désire montrer l'existence d'une décomposition :

(2) $A = D + N$, avec D, N polynômes en A à coefficients dans K, D diagonalisable **dans** $\mathbb{C}$, N nilpotente.

A noter que cela entraîne $DN = ND$ et le fait que D et N sont à coefficients dans le même corps K que la matrice A.
On rappelle qu'un polynôme $R \in K[X]$ est irréductible s'il n'est pas constant et si ses seuls diviseurs sont les constantes et les polynômes λR avec $\lambda \in K^*$; tout polynôme de $K[X]$ s'écrit de manière essentiellement unique comme un produit de polynômes irréductibles de $K[X]$.
On dit qu'un polynôme à coefficients dans K, de degré ≥ 1, est sans facteur carré s'il est produit de polynômes irrréductibles distincts c'est-à-dire si les exposants intervenant dans sa décomposition primaire sont tous égaux à 1.

1. Soit $\chi \in K[X]$ de degré ≥ 1 ; montrer l'existence et l'unicité d'un polynôme $P \in K[X]$, unitaire, sans facteur carré, tel que :

$$P \text{ divise } \chi, \quad \chi \text{ divise une puissance de } P.$$

Montrer qu'un polynôme à coefficients dans K sous-corps de $\mathbb{C}$ est sans facteur carré si et seulement si il est premier avec sa dérivée. En déduire une expression de P en fonction de χ et $\mathrm{pgcd}(\chi, \chi')$.

2. On désigne maintenant par χ le polynôme caractéristique de la matrice A et par P le polynôme intervenant dans la question précédente. Montrer qu'une matrice annulée par le polynôme P est diagonalisable dans $\mathbb{C}$.

3. On raisonne dans le sous-anneau (commutatif) $\mathbf{A} \subset \mathrm{M}_n(K)$ constitué des matrices de la forme $Q(A)$ avec $Q \in K[X]$ et on pose $B = P(A)$. Montrer, dans cet anneau, que $P'(A)$ est inversible modulo B ; comment calculer un inverse de $P'(A)$ modulo B ?

4. Construire une suite de matrices $(A_i)_{i\geq 1}$ telle que :

$$A_i \in \mathbf{A}, \quad P(A_i) \equiv 0 \pmod{B^i}, \quad A_i \equiv A \pmod{B}$$

En remarquant que B est nilpotente, montrer l'existence d'une décomposition **(2)**.

5. Montrer qu'en fait pour tout polynôme sans facteur carré P à coefficients dans K (K désigne toujours un sous-corps de $\mathbb{C}$), on peut définir une suite de polynômes $(Q_i)_{i\geq 1}$ telle que :

$$P(Q_i(X)) \equiv 0 \pmod{P^i}, \quad Q_i(X) \equiv X \pmod{P}.$$

En déduire de nouveau l'existence d'une décomposition **(2)**.