10.05M

SESSION 2010

Filière MP (groupe I)

Épreuve commune aux ENS de Paris, Lyon et Cachan

MATHÉMATIQUES – INFORMATIQUE

Durée : 4 heures

Les calculatrices ne sont pas autorisées.

Le sujet porte sur la résolution de systèmes d'équations linéaires dans les entiers. La première partie traite de la résolution d'une équation dans $\mathbb{Z}$. La seconde partie étudie la résolution d'un système d'équations dans $\mathbb{N}$. La troisième partie porte sur le nombre de Frobenius. La quatrième et dernière partie est consacrée à l'étude d'une borne inférieure sur le nombre de Frobenius. Les quatre parties sont largement indépendantes. En particulier, la deuxième partie est indépendante des autres.

L'usage des calculatrices est interdit.

Préambule

$\mathbb{Z}$ représente l'ensemble des entiers relatifs, $\mathbb{N}$ l'ensemble des entiers positifs, $\mathbb{N}^*$ l'ensemble des entiers strictement positifs et $\mathbb{R}$ l'ensemble des réels. Soient a, b, d des entiers relatifs, d non nul. On dit que d *divise* a s'il existe $k \in \mathbb{Z}$ tel que $a = kd$. Le *plus grand diviseur commun* de a et b, noté $\mathsf{pgcd}(a, b)$ est l'entier $d \geqslant 1$ tel que d divise a et d divise b et tel que pour tout diviseur d' de a et b, d' divise d. Plus généralement, étant donnés $a_1, \ldots, a_n \in \mathbb{Z}$, le *plus grand diviseur commun* des a_i, $1 \leqslant i \leqslant n$, noté $\mathsf{pgcd}(a_1, \ldots, a_n)$ est l'entier $d \geqslant 1$ tel que d divise chacun des a_i, $1 \leqslant i \leqslant n$, et tel que pour tout diviseur d' de chacun des a_i, d' divise d.

Si A est une matrice de taille $m \times k$, le coefficient (i, j), où i est l'indice de ligne et j l'indice de colonne, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant k$, de la matrice A est noté $A_{i,j}$. Si u est un vecteur de taille k, la $i$ème coordonnée de u, $1 \leqslant i \leqslant k$, est notée u_i. La matrice identité de taille $k \times k$ est notée I_k. Une matrice de taille $1 \times k$ pourra être appelée vecteur même si ses coefficients ne sont pas dans un corps.

Si A et B sont deux ensembles, on note $A \setminus B$ l'ensemble formé de A privé des éléments de B.

Algorithmes : certaines questions demandent de donner un algorithme. Pour ces questions, on ne demande pas de fournir du pseudo-code mais de décrire l'algorithme en français. La question 2.5 illustre une présentation possible.

TOURNEZ LA PAGE S.V.P.

PARTIE 1 : Résolution d'une équation linéaire dans $\mathbb{Z}$

Étant donnés a, b deux entiers strictement positifs, on appelle *reste de la division euclidienne de a par b*, noté $r(a,b)$ l'entier r tel que $0 \leqslant r < b$ et $a = kb + r$ pour un certain entier $k \in \mathbb{N}$. On rappelle que l'algorithme d'Euclide, permettant de calculer $\mathsf{pgcd}(a,b)$, est défini à l'aide des suites (u_n) et (v_n) de la manière suivante :

- $u_0 = a$ et $v_0 = b$
- Si $v_n \neq 0$, on définit $u_{n+1} = v_n$ et $v_{n+1} = r(u_n, v_n)$
- Si $v_n = 0$, alors l'algorithme s'arrête et renvoie u_n.

Question 1.1. Soit N l'indice tel que $v_N = 0$.

(a). Montrer que $u_N = \mathsf{pgcd}(a,b)$.

(b). Montrer qu'il existe $p, q \in \mathbb{Z}$ tels que $u_N = ap + bq$.

Soient $a_1, \ldots, a_n \in \mathbb{Z}$, $b \in \mathbb{Z}$ des entiers relatifs. On dit que l'équation

$$a_1x_1 + \ldots + a_nx_n = b$$

a une solution dans $\mathbb{Z}$ s'il existe $u_1, \ldots, u_n \in \mathbb{Z}$ tels que $a_1u_1 + \ldots + a_nu_n = b$.

Question 1.2. Soient $a_1, \ldots, a_n \in \mathbb{Z}$, $n \geqslant 2$ et $b \in \mathbb{Z}$. Soit $a' = \mathsf{pgcd}(a_1, a_2)$. Montrer que l'équation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ a une solution dans $\mathbb{Z}$ si et seulement si l'équation $a'x' + a_3x_3 + \ldots + a_nx_n = b$ a une solution dans $\mathbb{Z}$. En déduire que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ a une solution dans $\mathbb{Z}$ si et seulement si $\mathsf{pgcd}(a_1, \ldots, a_n)$ divise b.

En particulier, l'équation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = \mathsf{pgcd}(a_1, \ldots, a_n)$ a toujours une solution dans $\mathbb{Z}$ (théorème de Bézout).

Question 1.3. Proposer un algorithme qui prend en entrée une équation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ et renvoie :

- "pas de solution" s'il n'y a pas de solution dans $\mathbb{Z}$,
- donne une solution (dans $\mathbb{Z}$) lorsqu'il en existe une.

On supposera donnée une fonction $\mathsf{pgcd}_{\mathsf{et}}$ qui prend en entrée deux entiers $a, b \in \mathbb{N}$ et qui renvoie d, p, q tels que $d = pa + qb$ et $d = \mathsf{pgcd}(a,b)$.

Question 1.4. Trouver une solution dans $\mathbb{Z}$ de l'équation $10x_1 - 15x_2 + 7x_3 = 3$.

PARTIE 2 : Base des solutions dans $\mathbb{N}$ d'un système d'équations linéaires

Soit A une matrice de taille $m \times k$ à coefficients dans $\mathbb{Z}$. L'ensemble des *solutions dans* $\mathbb{N}$ de l'équation $AX = 0$, noté $S(A)$, est l'ensemble des vecteurs $X \in \mathbb{N}^k$ tels que $AX = 0$. Une *base* de $S(A)$ est un ensemble de vecteurs de $\mathbb{N}^k$ tel que tout vecteur de $S(A)$ s'écrive comme une combinaison linéaire à coefficients *entiers positifs* d'éléments de la base.

Étant donnés deux vecteurs $U, V \in \mathbb{N}^k$, on écrit $U \leqslant V$ si et seulement si $U_i \leqslant V_i$ pour tout $1 \leqslant i \leqslant k$.

Question 2.1. Montrer que la relation $\leqslant$ est un ordre sur les vecteurs de $\mathbb{N}^k$.

On considère l'ensemble $H(A)$ des solutions non nulles dans $\mathbb{N}$ de l'équation $AX = 0$, minimales pour l'ordre $\leqslant$, c'est-à-dire

$$H(A) = \{X \in S(A), X \neq 0 \mid (Y \in S(A) \text{ et } Y \leqslant X) \Rightarrow (Y = X \text{ ou } Y = 0)\}.$$

Question 2.2. Montrer que $H(A)$ est fini.

Question 2.3. Montrer que $H(A)$ est une base de $S(A)$.

Question 2.4. Montrer que toute base de $S(A)$ contient $H(A)$.

On s'intéresse à la détermination de $H(A)$. Une *contrainte* est un triplet formé d'une matrice M carrée de taille $k \times k$ à coefficients dans $\mathbb{N}$, d'une matrice A de taille $m \times k$ à coefficients dans $\mathbb{Z}$ et d'un ensemble $I \subseteq \{1, \ldots, k\}$.

La contrainte associée à (M, A, I) est notée $C(M, A, I)$. L'ensemble des solutions, noté $Sol(C(M, A, I))$, d'une contrainte $C(M, A, I)$ est défini par

$$Sol(C(M, A, I)) = \{Mu \mid Au = 0 \text{ et } u \in \mathbb{N}^k \text{ et } \forall i \in I,\ u_i = 0\}.$$

Ainsi $S(A)$ est l'ensemble des solutions de la contrainte $C(\mathsf{Id}_k, A, \emptyset)$. Par convention, on appellera matrice vide la matrice de taille $0 \times k$, notée ϵ. L'ensemble des solutions, noté $Sol(C(M, \epsilon, I))$, associé à $C(M, \epsilon, I)$ est défini par

$$Sol(C(M, \epsilon, I)) = \{Mu \mid u \in \mathbb{N}^k \text{ et } \forall i \in I,\ u_i = 0\}.$$

On dit qu'une contrainte $C(M, A, I)$ est *en forme résolue* si A est la matrice vide. Étant donné un ensemble E de contraintes, l'ensemble des solutions de E est $Sol(E) = \cup_{C \in E} Sol(C)$.

On définit $L_{i,j}$ la matrice carrée telle que le coefficient (p, q) de $L_{i,j}$ vaut 1 si $p = q$ ou si $(p, q) = (i, j)$ et vaut 0 sinon.

Nous allons étudier un algorithme Transf décrit ci-dessous, qui transforme un ensemble de contraintes en un ensemble de contraintes en forme résolue.

Transf(E) =
  E si pour tout $C \in E$, C est en forme résolue.
  Sinon, choisir $C(M, A, I) \in E$ qui n'est pas en forme résolue.
    Si les $A_{1,i}$, $i \notin I$ ne sont pas tous de même signe,
      choisir $i, j \notin I$ tels que $A_{1,i}A_{1,j} = \min_{p,q} A_{1,p}A_{1,q} < 0$;
      calculer Transf $((E \setminus \{C(M, A, I)\}) \cup \{C(ML_{i,j}, AL_{i,j}, I), C(ML_{j,i}, AL_{j,i}, I)\})$.
    Sinon, soit $A_{1,*}$ la première ligne de A. On peut écrire A sous la forme $A = \begin{bmatrix} A_{1,*} \\ A' \end{bmatrix}$.
      Soit $I' = I \cup \{j \mid A_{1,j} \neq 0\}$.
      Calculer Transf$((E \setminus \{C(M, A, I)\}) \cup \{C(M, A', I')\})$.

Question 2.5. Soit E un ensemble fini de contraintes. Montrer que Transf(E) renvoie toujours un résultat en un nombre fini d'étapes.

Question 2.6. Montrer que si E est un ensemble de contraintes et Transf$(E) = E'$ alors $Sol(E) = Sol(E')$.

Question 2.7. En déduire un algorithme pour déterminer $H(A)$.

Question 2.8. Soit $A = \begin{bmatrix} 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & -3 \end{bmatrix}$. Déterminer $H(A)$.

TOURNEZ LA PAGE S.V.P.

PARTIE 3 : Problème de Frobenius

Dans cette partie, on suppose que $a_1, \ldots, a_n \in \mathbb{N}$ sont des entiers positifs tels que $a_i \geqslant 2$, $1 \leqslant i \leqslant n$. On dit qu'un entier b est *représentable* comme une combinaison linéaire positive de $a_1, \ldots, a_n$ s'il existe des entiers $x_i \geqslant 0$, $1 \leqslant i \leqslant n$, tels que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$.

Question 3.1. Soit b un entier. Les deux propositions suivantes sont-elles équivalentes ? Justifier la réponse.

i) b est représentable comme une combinaison linéaire positive de $a_1, \ldots, a_n$.

ii) $\mathsf{pgcd}(a_1, \ldots, a_n)$ divise b.

Question 3.2. On suppose $\mathsf{pgcd}(a_1, \ldots, a_n) = 1$. Montrer qu'il existe un entier N tel que pour tout entier $b \geqslant N$, b est représentable comme une combinaison linéaire positive de $a_1, \ldots, a_n$.

On suppose désormais que $\mathsf{pgcd}(a_1, \ldots, a_n) = 1$. On note $g(a_1, \ldots, a_n)$ le plus grand entier non représentable comme combinaison linéaire positive de $a_1, \ldots, a_n$. Le nombre $g(a_1, \ldots, a_n)$ est appelé *nombre de Frobenius*.

Question 3.3. Soient $a, b \geqslant 2$, $\mathsf{pgcd}(a, b) = 1$. Soit T l'ensemble des entiers représentables comme une combinaison linéaire positive de a et b.

(a). Montrer que $ab - a - b \notin T$.

(b). Montrer que pour tout entier k, il existe $v_1 \in \mathbb{Z}$ et $v_2 \in \mathbb{N}$ tel que $v_2 < a$ et $k = v_1a + v_2b$.

(c). Montrer que pour tout entier $i \geqslant 1$, $ab - a - b + i \in T$.

(d). En déduire que le nombre de Frobenius associé à a et b est $g(a, b) = ab - a - b$.

Soient $a, b, c \in \mathbb{Z}$. On dit que a est *congru* à b modulo c, noté $a \equiv b \mod c$, s'il existe $k \in \mathbb{Z}$ tel que $a = b + ck$.

Question 3.4. Soient $a_1, \ldots, a_n \in \mathbb{N}$, $n \geqslant 2$ des entiers positifs. Pour tout $\ell \in \mathbb{N}$, on définit t_ℓ le plus petit entier positif congru à ℓ modulo a_n et représentable comme une combinaison linéaire positive de $a_1, \ldots, a_{n-1}$. Montrer que

$$g(a_1, \ldots, a_n) + a_n = \max_{\ell \in \{0, \ldots, a_n - 1\}} \{t_\ell\}.$$

Si A et B sont deux parties de $\mathbb{R}^d$, l'ensemble $A + B$ est l'ensemble des $u + v$ avec $u \in A$ et $v \in B$. Si t est un réel, tA est l'ensemble des tu, $u \in A$. S'il existe un réel positif t tel que $\mathbb{R}^d = tA + B$, on définit le *rayon couvrant* de A par rapport à B par

$$\mu(A, B) = \inf\{t \in \mathbb{R}^+ \mid \mathbb{R}^d = tA + B\}.$$

On considère $L = \{(x_1, \ldots, x_{n-1}) \mid x_i \in \mathbb{Z} \text{ et } \sum_{i=1}^{n-1} a_i x_i \equiv 0 \mod a_n\}$ et $S = \{(x_1, \ldots, x_{n-1}) \mid x_i \in \mathbb{R}, x_i \geqslant 0 \text{ et } \sum_{i=1}^{n-1} a_i x_i \leqslant 1\}$.

Question 3.5. Montrer que $\mathbb{Z}^{n-1} \subseteq (g(a_1, \ldots, a_n) + a_n)S + L$.

Question 3.6. Montrer que $\mu(S, L)$ existe et que $\mu(S, L) \leqslant g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$.

Question 3.7. Montrer que $g(a_1, \ldots, a_n) + a_n$ est le plus petit réel positif t tel que $tS + L$ contienne $\mathbb{Z}^{n-1}$.

Question 3.8. Montrer que $\mu(S, L) = g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$.

PARTIE 4 : Dénumérants et borne inférieure sur le nombre de Frobenius

On considère $a_1, \ldots, a_n \in \mathbb{N}^*$ et $m \in \mathbb{N}^*$ des entiers strictement positifs. Le *dénumérant* $d(m, a_1, \ldots, a_n)$ est le nombre de solutions dans $\mathbb{N}$ de l'équation $\sum_{i=1}^n a_i x_i = m$, c'est-à-dire le cardinal de l'ensemble

$$\{(x_1, \ldots, x_n) \mid x_i \in \mathbb{N} \text{ et } \sum_{i=1}^{n} a_i x_i = m\}.$$

On considère la fonction $f :]-1, 1[\to \mathbb{R}$ définie par

$$f(x) = \frac{1}{(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})}.$$

Question 4.1. Montrer que f est développable en série entière et que son développement est $f(x) = \sum_{i=0}^{\infty} d(i, a_1, \ldots, a_n) x^i$.

Question 4.2. Donner une formule explicite pour $d(m, 1, 2)$.

On suppose désormais fixés $a_1, \ldots, a_n \in \mathbb{N}^*$ des entiers strictement positifs.

Étant donnés $b_1, \ldots, b_n \in \mathbb{N}$, on considère $B(b_1, \ldots, b_n)$ le rectangle n-dimensionnel formé de l'ensemble des points $x \in \mathbb{R}^n$ tels que $b_i a_i \leqslant x_i < (b_i + 1)a_i$. Étant donné $r \in \mathbb{R}^+$, on considère la pyramide $P(r)$ formée de l'ensemble des vecteurs $x \in (\mathbb{R}^+)^n$ tels que $x_1 + \cdots + x_n \leqslant r$.

Question 4.3. Montrer que $P(m) \subseteq \bigcup_{b_1 a_1 + \cdots + b_n a_n \leqslant m} B(b_1, \ldots, b_n)$.

On définit $d'(m, a_1, \ldots, a_n) = \sum_{i=0}^{m} d(i, a_1, \ldots, a_n)$, le nombre de solutions dans $\mathbb{N}$ de l'inégalité $\sum_{i=1}^n a_i x_i \leqslant m$.

On pose $p_n = \prod_{i=1}^n a_i$ et $s_n = \sum_{i=1}^n a_i$.

Question 4.4. Montrer que $\frac{m^n}{n! p_n} \leqslant d'(m, a_1, \ldots, a_n) \leqslant \frac{(m+s_n)^n}{n! p_n}$.

On pose $g_n = g(a_1, \ldots, a_n)$.

Question 4.5. On considère la fonction $f :]0, +\infty[\to]0, +\infty[$ définie par $f(y) = \frac{(y+g_n+s_n)^n}{y}$. Montrer que $f(y) > n! p_n$.

Question 4.6. Montrer que $g(a_1, \ldots, a_n) \geqslant \frac{n-1}{n}\left((n-1)! \prod_{i=1}^n a_i\right)^{\frac{1}{n-1}} - \sum_{i=1}^n a_i$.

Fin de l'épreuve.