ÉPREUVE ÉCRITE DE MATHS-INFO

CONCOURS INTER-ENS

MEMBRES DE JURYS : N. Brisebarre, V. Cortier et Ph. Duchon

Le sujet portait sur la résolution d'équations Diophantiennes linéaires, c'est-à-dire la recherche de solutions à coefficients entiers positifs (sauf pour la première partie) de systèmes d'équations linéaires.

Plus précisément, la première partie montrait comme calculer une solution (dans $\mathbb{Z}$) d'une équation linéaire en éliminant peu à peu les variables à l'aide de l'algorithme d'Euclide pour le calcul du PGCD. La deuxième partie permettait de montrer que, dans le cas d'un système d'équations linéaires, il est possible d'exprimer toutes les solutions comme combinaisons linéaires d'un ensemble fini de solutions (minimales), appelé *base*. Un algorithme[1] était proposé pour calculer une telle base. La preuve de la terminaison et de la correction de cet algorithme constituait le noyau dur de cette deuxième partie.

Les troisièmes et quatrièmes parties portaient sur le *nombre de Frobenius*, c'est-à-dire, étant donnés $a_1, \ldots, a_n$ dans $\mathbb{N}^*$, premiers entre eux, l'entier b à partir duquel l'équation $\sum_{i=1}^{n} a_i x_i = b$ admet toujours une solution dans $\mathbb{N}^n$. Savoir si on peut écrire un entier comme une combinaison linéaire d'autres entiers donnés est une question qui apparaît dans différents problèmes comme par exemple le rendu de monnaie : Étant données n types de pièces chacune de valeur a_i, pour quelles valeurs n'est-il pas possible de rendre la monnaie ? La troisième partie montrait l'existence du nombre de Frobenius pour tous entiers $a_1, \ldots, a_n$ et donnait une expression du nombre de Frobenius pour les équations linéaires à deux variables. La fin de la troisième partie permettait de caractériser, dans le cas général, le nombre de Frobenius à l'aide du rayon couvrant (caractérisation à l'origine d'un algorithme de calcul du nombre de Frobenius). La quatrième partie calculait une borne inférieure pour le nombre de Frobenius en passant par la notion de *dénumérant*, à savoir le nombre de solutions de l'équation $\sum_{i=1}^{n} a_i x_i = b$. Ces deux dernières parties sont inspirées du livre « The Diophantine Frobenius Problem »[2].

Remarques générales

La première partie (courte et facile) avait pour but de familiariser les candidats avec des raisonnements élémentaires d'arithmétique. Toutes les copies l'ont abordée. Cependant, s'il est acceptable de ne pas démontrer une hypothèse de récurrence correctement énoncée et trivialement vraie, les raisonnements utilisant des points de suspension ou des phrases de la forme « en itérant le processus, on voit que ... » ont fait perdre des points aux candidats.

[1] tiré de l'article de E. Domenjoud et A. Paula Tomás : From Elliott-MacMahon to an Algorithm for General Linear Constraints on Naturals. *Principles and Practice of Constraint Programming (CP 1995)*, LNCS, volume 976, pages 18-35.

[2] J.L. Ramírez Alfonsín, The Diophantine Frobenius Problem, *Oxford Lectures Series in Mathematics and its Applications*, Oxford University Press, (2005).

Les deuxième et troisième parties étaient très différentes l'une de l'autre et la plupart des copies n'ont réellement abordé que l'une des deux parties, les meilleures copies s'attaquant aux deux. Les candidats n'ont pas touché à la quatrième et dernière partie (du moins avec succès) au delà de la question 4.2, excepté quelques rares copies qui ont traité également les questions 4.3 et 4.4.

Comme les années précédentes, il est rappelé aux candidats que la qualité de la rédaction est un critère important de la notation. Des affirmations non justifiées ne sont pas comptabilisées. Les arguments d'autorité de la forme « Il est clair que ... » ou « On voit donc bien que ... » ne convainquent pas les correcteurs.

Questions détaillées

Les paragraphes suivants commentent les réponses données aux questions les plus traitées.

Questions 1.1 et 1.2. Ces questions d'échauffement étaient faciles et ont été bien traitées, aux problèmes de rédaction près (mentionnés plus haut).

Question 1.3. Cette question n'a été parfaitement traitée que par un tiers des copies environ. Beaucoup de candidats ont du mal à formuler un algorithme. Si la terminologie et les structures de donnée utilisées sont laissées complètement libres, il importe que la réponse apportée soit bien un algorithme. Ainsi toutes les phrases vagues (mais fréquentes) de la forme « On itère le processus jusqu'à ce que $n = 1$ » ou « On remonte en utilisant les coefficients de Bezout », ne sont bien sûr par acceptées.

Question 1.4. Très bien traitée par presque toutes les copies dans la mesure où il suffisait d'exhiber une solution.

Question 2.1. 20% des copies ne connaissent pas la définition d'un ordre. En particulier, la notion de réflexivité est régulièrement oubliée.

Question 2.2. Très peu de copies ont réussi cette question. Beaucoup ont cherché à s'appuyer sur le fait que le noyau de A est de dimension finie, en oubliant que les coefficients devaient être positifs, comme l'indiquait clairement l'énoncé.

Question 2.3. Beaucoup de copies ont pensé à amorcer un raisonnement par récurrence : si $Y \in S(A)$ et $Y \notin H(A)$ alors $\exists X \leq Y$ tel que $X \in S(A)$ mais beaucoup ont directement affirmé que $X \in H(A)$. D'autre part, toutes les copies n'ont pas correctement justifié sur quoi était faite la récurrence (la somme des coordonnées par exemple). Enfin, certains ont été apparemment trompés par le terme de "base", qu'ils ont un peu hâtivement assimilé à celle de base (ensemble libre et générateur) d'un espace vectoriel. Il faut veiller à bien lire les définitions de l'énoncé.

Question 2.4. Cette question a été bien traitée par une majorité de copies.

Question 2.5. Cette question a été abordée par un grand nombre de copies mais rarement avec succès. Elle a souvent donné lieu à plus d'une page de rédaction.

Question 2.6. Peu de copies ont abordé cette question qui se résolvait pourtant plutôt facilement en s'y prenant tranquillement et en faisant attention à la positivité des coefficients.

Question 2.7. Les copies qui ont abordé cette question ne savaient en général pas comment extraire les solutions minimales de $\mathsf{Transf}(\{C(\mathsf{Id}_k, A, \emptyset)\})$.

Question 2.8. Itérer l'algorithme sur l'entrée donnée demandait de trouver une représentation astucieuse des données, ce qu'aucune copie n'a fait. Plusieurs copies ont cependant calculé $H(A)$ par d'autres moyens, ce qui a été partiellement récompensé.

Question 3.1. Un contre-exemple a été fourni dans presque toutes les copies.

Question 3.2. Beaucoup de copies ont su traiter cette question, quitte à exhiber des bornes exubérantes (ce qui n'a bien sûr pas été sanctionné).

Question 3.3. Les propriétés à démontrer ont donné lieu à un certain nombre de tentatives d'arnaques ou au développement de longs calculs alors que chaque propriété pouvait se montrer en quelques lignes.

Questions 3.4 $\rightarrow$ 3.8. Ces questions ont été très peu abordées.

Question 4.1. La plupart des copies qui ont abordé cette question ont su justifier que f était développable en série entière. Par contre, le calcul du développement n'a pas toujours été bien traité.

Question 4.2. Les copies qui ont traité cette question l'ont en général fait sans passer par les séries entières mais en calculant $d(m, 1, 2)$ directement à partir de sa définition.

Question 4.3. Cette question était plutôt facile et a été bien traitée par les candidats qui sont allés jusque-là.

Question 4.4. Une seule copie a obtenu des points à cette question.

Questions 4.5 $\rightarrow$ 4.6. La fin du problème n'a pas été abordée, du moins avec succès.

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.

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 $u_N = ap + bq$.

C'est probablement du cours. a) On montre que $\mathsf{pgcd}(u_n, v_n) = \mathsf{pgcd}(u_{n+1}, v_{n+1})$ et donc par récurrence $u_N = \mathsf{pgcd}(a,b)$. b) On montre par récurrence que u_n et v_n s'écrivent comme combinaison linéaire (à coefficients entiers) de a et b.

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.

a' divise a_1 donc $a_1 = k_1a'$. De même $a_2 = k_2a'$. Soit $(e_1, e_2, e_3, \ldots, e_n) \in \mathbb{Z}^n$ une solution de l'équation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$. On pose $e' = k_1e_1 + k_2e_2$. On vérifie que $e', e_3, \ldots, e_n$ est une solution de l'équation $a'x' + a_3x_3 + \ldots + a_nx_n = b$.

Réciproquement, $a' = \mathsf{pgcd}(a_1, a_2)$ donc il existe p, q tels que $a' = a_1p + a_2q$ (cf question précédente). Soit $e', e_3, \ldots, e_n$ une solution de l'équation $a'x' + a_3x_3 + \ldots + a_nx_n = b$. On pose $e_1 = pe'$ et $e_2 = qe'$. On a que $e_1, e_2, e_3, \ldots, e_n$ est une solution de l'équation $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$. On déduit par récurrence 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 remarquant que $\mathsf{pgcd}(a_1, \ldots, a_n) = \mathsf{pgcd}(\mathsf{pgcd}(a_1, a_2), a_3, \ldots, a_n)$.

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 $d = \mathsf{pgcd}(a,b)$.

On réduit le nombre d'inconnues en utilisant la question précédente. L'algorithme se définit facilement de manière récursive.

Solve$(a_1x_1 + a_2x_2 + \ldots + a_nx_n = b) =$
    Si $n = 1$ *alors*
        si a_1 *divise* b *alors* $\frac{b}{a_1}$

sinon "pas de solution".
Sinon $(n \geqslant 2)$
soit $(a', p, q) = \mathsf{pgcd}_{\mathsf{et}}(a_1, a_2)$
si $Solve(a'x' + a_3x_3 + \ldots + a_nx_n = b)$ *renvoie "pas de solution" alors "pas de solution"*
sinon, soit $(e', e_3, \ldots, e_n)$ *la solution donnée par* $Solve(a'x' + a_3x_3 + \ldots + a_nx_n = b)$
on retourne $(pe', qe', e_3, \ldots, e_n)$

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

D'après la question précédente, $10x_1 - 15x_2 + 7x_3 = 3$ a une solution ssi $5x'_2 + 7x_3 = 3$ a une solution car $\mathsf{pgcd}(10, 15) = 5$. Or $5x'_2 + 7x_3 = 3$ a une solution ssi $x'_3 = 3$ a une solution car $\mathsf{pgcd}(5, 7) = 1$. On remarque que $x'_3 = 3$ admet une solution. Il faut maintenant remonter. On a $1 = 3 * 5 - 2 * 7$ donc $3 = 9 * 5 - 6 * 7$ donc $x_2 = 9$ et $x_3 = -6$ est une solution de $5x'_2 + 7x_3 = 3$. De plus, $5 = -10 + 15$ donc $3 = 9 * (-10 + 15) - 6 * 7$ et donc $x_1 = -9$, $x_2 = 9$ et $x_3 = -6$ est une solution 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 vérifie (trivialement) réflexivité, antisymétrie et transitivité.

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.

Par contradiction. Si $H(A)$ est infini, on ordonne $H(A)$ en une suite infinie, croissante sur la première composante, de laquelle on extrait une sous-suite infinie croissante sur la deuxième composante, etc. On obtient ainsi une sous-suite croissante infinie pour l'ordre $\leqslant$, ce qui contredit la minimalité des éléments de $H(A)$.

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

On montre par récurrence sur la taille de $X \in S(A)$ (notée $|X|$ et définie comme la somme des coefficients) que X est une combinaison linéaire à coefficients entiers positifs d'éléments de $H(A)$. Soit $X \in S(A)$. Si $X \in H(A)$, la propriété est démontrée. Sinon, X n'est pas minimal dans $S(A)$ donc il existe $Y \in S(A)$ tel que $Y \leqslant X$ et $|Y| < |X|$. Par hypothèse de récurrence, Y est une combinaison linéaire à coefficients entiers positifs d'éléments de $H(A)$. Soit $Z = X - Y$. On a $|Z| < |X|$, $Z \in \mathbb{N}^k$ et $AZ = 0$ donc $Z \in S(A)$. Par hypothèse de récurrence, Z est une combinaison linéaire à coefficients entiers positifs d'éléments de $H(A)$. On en déduit que $X = Y + Z$ est une combinaison linéaire à coefficients entiers positifs d'éléments de $H(A)$.

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

Soit B une base de $S(A)$ et soit $X \in H(A)$. $X = \sum_{i=1}^{n} k_i U_i$ avec $U_i \in B$ et $k_i \in \mathbb{N}^*$. La minimalité de X assure que $n = 1$ et $k_1 = 1$ c'est-à-dire $X \in B$.

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.

On remarque que si $A_{1,i}A_{1,j} < 0$ alors après transformation le min des produits $A_{1,p}A_{1,q}$, $p, q \in I$, augmente strictement donc les règles suivantes finissent par être appliquées ce qui diminue strictement la taille des matrices.

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

On montre que la transformation préserve l'ensemble des solutions pas à pas. On note e_i les vecteurs de la base canonique de $\mathbb{R}^k$.

1er cas : Montrons que $Sol(C(M, A, I)) = Sol(C(ML_{i,j}, AL_{i,j}, I)) \cup Sol(C(ML_{j,i}, AL_{j,i}, I))$ pour $i, j \notin I$. Soit v tel que $v = Mu$, $Au = 0$, $u \in \mathbb{N}^k$, $u_p = 0$ pour $p \in I$. On a $u_i \geqslant u_j$ ou bien $u_j \geqslant u_i$. On

suppose par exemple que $u_i \geqslant u_j$. Soit $u' = u - u_j e_i$. On a $u' \in \mathbb{N}^k$, $u'_p = 0$ pour $p \in I$ et $L_{i,j}u' = u$ d'où $v = ML_{i,j}u'$ et donc $v \in C(ML_{i,j}, AL_{i,j}, I)$. Réciproquement, si $v = ML_{i,j}u'$ avec $AL_{i,j}u' = 0$ et $u'_p = 0$ pour $p \in I$. Soit $u = L_{i,j}u'$. On a $u \in \mathbb{N}^k$ et $u_p = 0$ pour $p \in I$ car $p \neq i, j$ d'où $v \in Sol(C(M, A, I))$.

2ème cas : Soit $A = \begin{bmatrix} A_{1,*} \\ A' \end{bmatrix}$ avec les L_i, $i \notin I$ tous du même signe et $I' = I \cup \{j \mid A_{1,j} \neq 0\}$. Montrons que $Sol(C(M, A, I)) = Sol(C(M, A', I'))$. Soit $v = Mu$, $Au = 0$, $u \in \mathbb{N}^k$, $u_p = 0$ pour $p \in I$. Alors $A'u = 0$ et $A_{1,*}u = 0$ garantit $u_p = 0$ pour $p \in I'$, d'où $v \in Sol(C(M, A', I'))$. Réciproquement, soit $v = Mu$, $A'u = 0$, $u \in \mathbb{N}^k$, $u_p = 0$ pour $p \in I'$. Alors $A_{1,*}u = 0$ d'où $v \in Sol(C(M, A, I))$.

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

On applique l'algorithme Transf sur le singleton $\{C(\mathsf{Id}_k, A, \emptyset)\}$. On obtient

$$\mathsf{Transf}(\{C(\mathsf{Id}_k, A, \emptyset)\}) = \{C(M_1, \epsilon, I_1), \ldots, C(M_n, \epsilon, I_n)\}$$

où ϵ est la matrice vide (de taille $0 \times k$). Alors $H(A)$ est contenu dans les vecteurs colonnes $M_i e_j$, $j \notin I_i$. Il suffit de retirer les vecteurs qui ne sont pas minimaux pour déduire $H(A)$.

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

En appliquant l'algorithme, on trouve $H(A) = \left\{ \begin{bmatrix} 1 \\ 1 \\ 2 \\ 1 \end{bmatrix}, \begin{bmatrix} 2 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 3 \\ 1 \end{bmatrix}, \begin{bmatrix} 3 \\ 1 \\ 0 \\ 1 \end{bmatrix} \right\}$. La figure en dernière page représente les pas de l'algorithme. On représente une contrainte $C(M, A, I)$ par la matrice $\left[\begin{array}{c} \mathrm{A} \\ \hline \mathrm{M} \end{array}\right]$ où les colonnes d'indice dans I sont rayées puis oubliées. Les contraintes sans solution (coefficients tous de même signe) ont été omises. Les coefficients choisis pour pivoter sont entourés en rouge et les vecteurs de la base sont entourés en bleu. On vérifie qu'ils sont minimaux. On peut remarquer qu'on obtient les mêmes vecteurs plusieurs fois, l'algorithme n'est pas très efficace.

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.

On attend un contre-exemple. Par exemple $2x_1+3x_2 = 1$ n'a pas de solution dans $\mathbb{N}$ alors que $\mathsf{pgcd}(2, 3) = 1$ divise 1.

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 $a_1, \ldots, a_n$.

Comme $\mathsf{pgcd}(a_1, \ldots, a_n) = 1$, il existe des entiers $x_i \in \mathbb{Z}$ tels que $a_1x_1 + a_2x_2 + \ldots + a_nx_n = 1$ (cf question 1.2). On groupe la somme sous la forme $P - Q = 1$, avec P et Q, combinaisons linéaires positives de $a_1, \ldots, a_n$. Soit $k \geqslant 0$. k s'écrit sous la forme $k = ha_1 + k'$ avec $h \geqslant 0$ et $0 \leqslant k' < a_1$. On a $(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k'(P - Q) = (a_1 - 1 - k')Q + ha_1 + k'P$ est une combinaison linéaire positive de $a_1, \ldots, a_n$. Donc tout entier supérieur à $(a_1 - 1)Q$ est représentable.

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 $g(a,b)=ab-a-b$.

(a). Supposons $ab-a-b\in T$. Écrivons $ab-a-b=r_1a+r_2b$, $r_1,r_2\in\mathbb{N}$. Alors $a(b-1-r_1)=b(1+r_2)$. On a donc $0<b-1-r_1<b$ et comme $\mathsf{pgcd}(a,b)=1$, on doit avoir que b divise $(b-1-r_1)$ ce qui contredit $0<b-1-r_1<b$.

(b). C'est probablement du cours. On sait déjà qu'il existe $v_1,v_2\in\mathbb{Z}$ tel que $k=v_1a+v_2b$. On écrit v_2 sous la forme $v_2=na+v_2'$ avec $0\leqslant v_2'<a$. On a alors $k=(v_1+n)a+v_2'b$.

(c). D'après (b), $ab-a-b+i=v_1a+v_2b$ avec $0\leqslant v_2<a$. On écrit $-i=(-v_1-1)a+(-v_2-1+a)b$. Comme $-i<0$ et $-v_2-1+a\geqslant 0$, on déduit $-v_1-1<0$, d'où $v_1\geqslant 0$.

(d). Conséquence de (a) et (c).

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

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

Soit L un entier positif. Si $L\equiv 0 \mod a_n$ alors L est une combinaison linéaire positive de a_n. Si $L\equiv\ell \mod a_n$ alors L est une combinaison linéaire positive de $a_1,\ldots,a_n$ si et seulement si $L\geqslant t_\ell$. Donc le plus grand entier congru à ℓ modulo a_n et non représentable sur les $a_1,\ldots,a_n$ est $t_\ell-a_n$. D'où le résultat.

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

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

Soit $y\in\mathbb{Z}^{n-1}$ et soit ℓ le reste de la division de $\sum_{i=1}^{n-1}a_iy_i$ par a_n. Alors $t_\ell=\ell+a_nx_n=\sum_{i=1}^{n-1}a_ix_i$ avec $x_i\geqslant 0$. Soit $x'=(x_1,\ldots,x_{n-1})$. On a $y-x'\in L$ et $y\in\{y-x'\}+t_\ell S$ puisque $x'\in t_\ell S$. D'après la question précédente, $t_\ell\leqslant g(a_1,\ldots,a_n)+a_n$, d'où $\mathbb{Z}^{n-1}\subseteq(g(a_1,\ldots,a_n)+a_n)S+L$.

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

On note $E(r)$ la partie entière de r. Si $x=(x_1,\ldots,x_n)$, on note $E(x)$ le vecteur $(E(x_1),\ldots,E(x_n))$. On remarque que pour $x\in\mathbb{R}^{n-1}$, $x-E(x)\in(a_1+\ldots+a_{n-1})S$. Donc $\mathbb{R}^{n-1}\subseteq\mathbb{Z}^{n-1}+(a_1+\ldots+a_{n-1})S$. En remarquant que $\lambda S+\mu S=(\lambda+\mu)S$, on déduit $\mathbb{R}^{n-1}\subseteq(g(a_1,\ldots,a_n)+a_1+\ldots+a_{n-1}+a_n)S+L$. D'où l'existence de $\mu(S,L)$ et l'inégalité recherchée.

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 $\mathbb{Z}^{n-1}$.

Par contradiction, supposons qu'il existe un réel $t < g(a_1, \ldots, a_n) + a_n$ tel que $tS + L$ contienne $\mathbb{Z}^{n-1}$. Soit $\ell \in \{0, \ldots, a_n - 1\}$ et $y \in \mathbb{Z}^{n-1}$ tel que $\sum_{i=1}^{n-1} a_i y_i \equiv \ell \mod a_n$. Alors il existe $x \in L$ tel que $y \in tS + x$, i.e. $y - x \in tS$. On remarque $\sum_{i=1}^{n-1} a_i(y_i - x_i) \equiv \ell \mod a_n$ et $y_i - x_i \geqslant 0$ car $y - x \in tS$. Donc $\sum_{i=1}^{n-1} a_i(y_i - x_i) \geqslant t_\ell$ et d'autre part $\sum_{i=1}^{n-1} a_i(y_i - x_i) \leqslant t$. On déduit $t_\ell \leqslant t$ pour tout ℓ, d'où (d'après la question 3.4), $g(a_1, \ldots, a_n) + a_n \leqslant t$, ce qui contredit $t < g(a_1, \ldots, a_n) + a_n$.

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

Il reste à montrer $\mu(S, L) \geqslant g(a_1, \ldots, a_n) + a_1 + \cdots + a_n$. D'après la question précédente, $g(a_1, \ldots, a_n) + a_n = \min\{t \in \mathbb{R}^+ \mid \mathbb{Z}^{n-1} \subseteq tS + L\}$. Donc il existe $y \in \mathbb{Z}^{n-1}$ tel que pour tout $x \in L$ tel que $y_i - x_i \geqslant 0$ pour tout i, on a $\sum_{i=1}^{n-1} a_i(y_i - x_i) \geqslant g(a_1, \ldots, a_n) + a_n$ (*). Soit $0 < \epsilon < 1$. On considère le point p défini par $p_i = y_i + \epsilon$. Soit $q \in L$ tel que $p_i \geqslant q_i$. Comme q_i est un entier, on a $y_i \geqslant q_i$.

On a donc $\sum_{i=1}^{n-1} a_i(p_i - q_i) = \epsilon \sum_{i=1}^{n-1} a_i + \sum_{i=1}^{n-1} a_i(y_i - q_i)$. D'où $\sum_{i=1}^{n-1} a_i(p_i - q_i) \geqslant \epsilon \sum_{i=1}^{n-1} a_i + g(a_1, \ldots, a_n) + a_n$ d'après (*). Donc $\mu(S, L) \geqslant \epsilon \sum_{i=1}^{n-1} a_i + g(a_1, \ldots, a_n) + a_n$ et donc $\mu(S, L) \geqslant \sum_{i=1}^{n-1} a_i + g(a_1, \ldots, a_n) + a_n$.

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 $f(x) = \sum_{i=0}^{\infty} d(i, a_1, \ldots, a_n) x^i$.

La fonction $x \mapsto \frac{1}{(1-x^r)}$ a pour développement en série entière $\sum_{i=0}^{\infty} x^{ri}$, de rayon de convergence 1. D'où $f(x) = \frac{1}{(1-x^{a_1})(1-x^{a_2})\cdots(1-x^{a_n})} = (\sum_{i_1=0}^{\infty} x^{a_1 i_1}) \cdots (\sum_{i_n=0}^{\infty} x^{a_n i_n}) = \sum_{i_1=0}^{\infty} \sum_{i_2=0}^{\infty} \cdots \sum_{i_n=0}^{\infty} x^{a_1 i_1 + \cdots + a_n i_n} = \sum_{i=0}^{\infty} d(i, a_1, \ldots, a_n) x^i$.

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

On cherche à développer la fonction $f(x) = \frac{1}{(1-x)(1-x^2)}$ en série entière. On a $f(x) = \frac{1}{4}\left(\frac{1}{1+x} + \frac{1}{1-x} + \frac{2}{(1-x)^2}\right)$. D'où $f(x) = \frac{1}{4}\left(\sum_{m=0}^{\infty} (-x)^m + \sum_{m=0}^{\infty} x^m + 2\sum_{m=0}^{\infty} (m+1)x^m\right)$. On déduit de la question précédente que $d(m, 1, 2) = \frac{1}{4}(2m + 3 + (-1)^m)$.

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

Tout point x de $P(m)$ appartient à un unique $B(b_1, \ldots, b_n)$ tel que $b_i a_i \leqslant x_i < (b_i + 1)a_i$, i.e. $b_i = E(\frac{x_i}{a_i})$. D'où $\sum_{i=1}^{n} b_i a_i = \sum_{i=1}^{n} E(\frac{x_i}{a_i}) a_i \leqslant \sum_{i=1}^{n} x_i \leqslant m$.

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

L'inégalité $\frac{m^n}{n! p_n} \leqslant d'(m, a_1, \ldots, a_n)$ est une conséquence directe de la question précédente en remarquant que le volume de $B(b_1, \ldots, b_n)$ est p_n et celui de $P(r)$ est $\frac{r^n}{n!}$ (on peut montrer ce dernier point par récurrence).

Pour l'autre inégalité, on commence par montrer que $\bigcup_{b_1 a_1 + \cdots + b_n a_n \leqslant m} B(b_1, \ldots, b_n) \subseteq P(m + \sum_{i=1}^{n} a_i)$. Pour tout point x de l'une des $d'(m, a_1, \ldots, a_n)$ boîtes $B(b_1, \ldots, b_n)$ qui satisfait $\sum_{i=1}^{n} b_i a_i \leqslant m$, on a $\sum_{i=1}^{n} x_i \leqslant \sum_{i=1}^{n} (b_i + 1) a_i \leqslant m + s_n$. Donc $x \in P(m + \sum_{i=1}^{n} a_i)$. On conclut à l'aide des volumes.

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 $f(y) > n! p_n$.

Soit $y \in]0, +\infty[$. On considère le nombre M de solutions de l'inégalité $\sum_{i=1}^{n} a_i x_i \leqslant g(a_1, \ldots, a_n) + y$. D'après la question précédente, on a $M \leqslant \frac{(g_n+y+s_n)^n}{n! p_n}$. D'autre part, par définition de $g(a_1, \ldots, a_n)$, tous les entiers $g_n + 1, \ldots, g_n + E(y)$ peuvent s'écrire comme $\sum_{i=1}^{n} a_i x_i$ avec $\sum_{i=1}^{n} a_i x_i \leqslant g(a_1, \ldots, a_n) + y$ et les vecteurs x sont distincts. Le vecteur 0 est également une solution distincte. Donc $M \geqslant E(y) + 1 > y$. On en déduit $f(y) > n! p_n$.

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

Le minimum de f sur $]0, +\infty[$ est atteint en $h = \frac{g_n+s_n}{n-1}$. On déduit de l'inégalité précédente que $f(h) = \frac{n^n (g_n+s_n)^{n-1}}{(n-1)^{n-1}} > n! p_n$. D'où $\frac{n^{n-1}(g_n+s_n)^{n-1}}{(n-1)^{n-1}} > (n-1)! p_n$ et le résultat.

Fin de l'épreuve.