Corrigé : épreuve de mathématiques-informatique ENS 2010

Les parties en italique sont des commentaires extraits du rapport du jury.

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.*
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.*

Partie 1. Résolution d'une équation linéaire dans $\mathbb{Z}$

Question 1.1 *Cette question et la suivante étaient faciles et ont été bien traitées, aux problèmes de rédaction près (mentionnés plus haut).*

(a) D'après le lemme d'Euclide, $\text{pgcd}(u,v) = \text{pgcd}(v, r(u,v))$ donc pour tout $n \in [\![0, \text{N}-1]\!]$, $\text{pgcd}(u_n, v_n) = \text{pgcd}(u_{n+1}, v_{n+1})$.
On en déduit par récurrence que $\text{pgcd}(a,b) = \text{pgcd}(u_\text{N}, 0) = u_\text{N}$.

(b) Montrons par récurrence descendante que pour tout $n \in [\![0, \text{N}]\!]$, il existe deux entiers p_n et q_n tels que $u_\text{N} = u_n p_n + v_n q_n$.
- Si $n = \text{N}$, il suffit de poser $p_\text{N} = 1$ et $q_\text{N} = 0$.
- Si $n < \text{N}$, on suppose l'existence de p_{n+1} et q_{n+1} vérifiant : $u_\text{N} = u_{n+1}p_{n+1} + v_{n+1}q_{n+1}$.
  On a $u_{n+1} = v_n$ et $v_{n+1} = u_n - kv_n$, où k est le quotient de la division euclidienne de u_n par v_n.
  Alors $u_\text{N} = v_n p_{n+1} + (u_n - kv_n)q_{n+1} = u_n q_{n+1} + v_n(p_{n+1} - kq_{n+1}) = u_n p_n + v_n q_n$.

En particulier pour $n = 0$ on obtient : $u_\text{N} = ap_0 + bq_0$.

Question 1.2 On raisonne par double application.

– Supposons que l'équation $a_1x_1 + a_2x_2 + \cdots a_nx_n = b$ ait une solution $(x_1, \ldots, x_n)$ dans $\mathbb{Z}^n$.
a' divise a_1 et a_2 donc il existe k_1 et k_2 dans $\mathbb{Z}$ tels que $a_1 = a'k_1$ et $a_2 = a'k_2$. Alors $b = a'(k_1x_1 + k_2x_2) + a_3x_3 + \cdots a_nx_n$.

– Réciproquement, supposons que l'équation $a'x' + a_3x_3 + \cdots + a_nx_n = b$ ait une solution dans $\mathbb{Z}$.
D'après la question précédente il existe p et q entiers tels que $a_1p + a_2q = a'$. Alors $b = a_1(px') + a_2(qx') + a_3x_3 + \cdots + a_nx_n = b$.

Montrons alors par récurrence sur n que l'équation $a_1x_1 + \cdots + a_nx_n = b$ a des solutions si et seulement si $\text{pgcd}(a_1, \ldots, a_n)$ divise b.
- Si $n = 1$, l'équation $a_1x_1 = b$ a bien des solutions si et seulement si a_1 divise b.
- Si $n > 1$, supposons le résultat acquis au rang $n-1$. D'après la première partie de cette question, $a_1x_1 + \cdots + a_nx_n = b$ a des solutions si et seulement si l'équation $a'x' + a_3x_3 + \cdots + a_nx_n = b$ en a, soit, par hypothèse de récurrence, si et seulement si $\text{pgcd}(a', a_3, \ldots, a_n)$ divise b. Or $\text{pgcd}(\text{pgcd}(a_1,a_2), a_3, \ldots, a_n) = \text{pgcd}(a_1, a_2, \ldots, a_n)$, d'où le résultat.

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 données 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 sur pas acceptées.*
On propose l'algorithme récursif suivant :

```
function RÉSOUDRE(a_1 x_1 + ··· + a_n x_n = b)
    if n = 1 then
        if a_1 divise b then return b/a_1
        else return "Pas de solution"
    else
        (a', p, q) = pgcd_et(a_1, a_2)
        if RÉSOUDRE(a'x' + ··· + a_n x_n = b) = "Pas de solution" then return "Pas de solution"
        else
            (x', x_3, ..., x_n) = RÉSOUDRE(a'x' + ··· + a_n x_n = b)
            return (px', qx', x_3, ..., x_n)
```

Question 1.4 *Très bien traitée par presque toutes les copies dans la mesure où il suffisait d'exhiber une solution.*
On applique l'algorithme précédent :
pgcd(10, 15) = 5 donc on cherche à résoudre $5x' + 7x_3 = 3$.
pgcd(5, 7) = 1 donc on cherche à résoudre $x'' = 3$, qui fournit une solution.
On a $5 \times 3 + 7 \times (-2) = 1$ donc $x' = 9$, $x_3 = -6$ est solution de $5x' + 7x_3 = 3$.
On a $10 \times (-1) - 15 \times (-1) = 5$ donc $x_1 = -9$, $x_2 = -9$, $x_3 = -6$ est solution de $10x_1 - 15x_2 + 7x_3 = 3$.

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

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

- La relation est réflexive car $U \leqslant U$: en effet, $U_i \leqslant U_i$ pour tout $1 \leqslant i \leqslant k$.
- La relation est anti-symétrique car $U \leqslant V$ et $V \leqslant U$ entraîne $U = V$: en effet, $U_i \leqslant V_i$ et $V_i \leqslant U_i$ pour tout $1 \leqslant i \leqslant k$.
- La relation est transitive car $U \leqslant V$ et $V \leqslant W$ entraîne $U \leqslant W$: en effet, $U_i \leqslant V_i \leqslant W_i$ pour tout $1 \leqslant i \leqslant k$.

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.*

Cette question repose sur le lemme suivant : « de toute suite à valeurs dans $\mathbb{N}$ on peut extraire une sous-suite croissante ». En effet, si cette suite n'est pas majorée c'est évident, et si elle est majorée elle possède une valeur d'adhérence et donc une sous-suite constante.

Raisonnons alors par l'absurde. Si H(A) était infini, il existerait une suite $(X_n)_{n\in\mathbb{N}}$ de solutions non nulles et deux-à-deux distinctes dans H(A).
De cette suite on peut extraire une sous-suite $(X_{\varphi_1(n)})_{n\in\mathbb{N}}$ croissante vis-à-vis de la première composante.
De cette sous-suite on peut extraire une sous-suite $(X_{\varphi_2\circ\varphi_1(n)})_{n\in\mathbb{N}}$ croissante vis-à-vis de la première et de la seconde composante.
En réitérant ce procédé on obtient une sous-suite $(X_{\varphi(n)})_{n\in\mathbb{N}}$ croissante vis-à-vis de chacune de ses composantes, autrement dit une sous-suite croissante pour la relation d'ordre sur $\mathbb{N}^k$.
Mais H(A) est constitué d'éléments minimaux pour cette relation d'ordre donc cette sous-suite doit être constante, ce qui est absurde puisque ces éléments ont été supposés deux-à-deux distincts.

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* $\exists X \leqslant Y$ *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.*

Soit $X \in S(A)$, et notons $|X|$ la somme des coordonnées de X. Nous allons montrer par récurrence sur $|X|$ que X s'exprime comme combinaison linéaire à coefficients positifs d'éléments de H(A).

- Si $|X| = 0$ alors $X = 0$ et le résultat est évident.
- Si $|X| > 0$, supposons le résultat acquis pour toute solution Y vérifiant $|Y| < |X|$.
  - Si $X \in H(A)$, le résultat est acquis.
  - Si $X \notin H(A)$, X n'est pas minimal donc il existe $Y \in S(A)$ tel que $Y \neq 0$ et $Y < X$.
    En particulier $|Y| < |X|$ donc Y est combinaison linéaire à coefficients positifs d'éléments de H(A).
    Posons $Z = X - Y$. Puisque $Y < X$ et $Y \neq 0$ on a $Z \in \mathbb{N}^k$ et $|Z| < |X|$. De plus, $AZ = AX - AY = 0$ donc $Z \in S(A)$. On peut donc à lui aussi appliquer l'hypothèse de récurrence : Z est combinaison linéaire à coefficients positifs d'éléments de H(A), et puisque $X = Y + Z$ il en est de même de X.

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

Soit B une base de S(A), et $X \in H(A)$. B est une base donc on peut écrire $X = \sum_{i=1}^{n} \lambda_i B_i$ avec $\lambda_i \in \mathbb{N}^*$ et $B_i \in B$.

Pour tout $1 \leqslant i \leqslant n$ on a $\lambda_i B_i \leqslant X$ et puisque X est minimal on a nécessairement $n = 1$ et $X = \lambda_1 B_1$. Or si $\lambda_1 \geqslant 2$ on a $B_1 < X$, ce qui ne se peut. Donc $X = B_1 \in B$. Toute base de S(A) contient H(A).

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.*
Si C(M, A, I) est une contrainte, on pose $|C(M,A,I)| = (m,\alpha)$ (le « poids » de la contrainte), où m est le nombre de lignes de A et $\alpha = -\min\left\{A_{1p}A_{1q} \;\middle|\; p,q \notin I \text{ et } A_{1p}A_{1q} < 0\right\}$ (avec la convention $\min\emptyset = 0$).
Si C et C′ sont deux contraintes, on note $C \preccurlyeq C'$ lorsque $m < m'$ ou $m = m'$ et $\alpha \leqslant \alpha'$, avec $|C| = (m,\alpha)$ et $|C'| = (m',\alpha')$. On définit ainsi un pré-ordre bien fondé sur l'ensemble des contraintes, c'est-à-dire que tout ensemble non vide possède un élément minimal.
Considérons maintenant une contrainte C(M, A, I) qui n'est pas sous forme résolue dans E.

- Si les A_{1i}, $i \notin I$ ne sont pas tous de même signe, le produit AL_{ij} remplace le coefficient A_{1j} par $A_{1j} + A_{1i}$ et laisse inchangés tous les autres coefficients de la première ligne. Compte tenu du choix de i et j, on a $|C(ML_{ij}, AL_{ij}, I)| \leqslant |C(M, A, I)|$, l'inégalité étant stricte lorsque α est atteint une seule fois, et le nombre de couples (i,j) atteignant α ayant diminué dans le cas contraire. Il en est de même pour $C(ML_{ji}, AL_{ji}, I)$.
- Si les A_{1i}, $i \notin I$ sont tous de même signe, alors $|C(M, A', I')| < |C(M, A, I)|$ puisque le nombre de lignes a diminué.

Ainsi, chaque appel récursif remplace une contrainte par une ou deux contraintes de poids inférieurs, ce qui assure la terminaison de la fonction puisqu'il n'y a pas d'appel récursif sur une contrainte de poids nul (c'est-à-dire sous forme résolue).

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.*
Considérons une contrainte C(M, A, I) qui n'est pas sous forme résolue dans E, et envisageons deux cas.

– Si les A_{1i}, $i \notin I$ ne sont pas tous de même signe, nous allons montrer que $Sol(C(M,A,I)) = Sol(C(ML_{ij}, AL_{ij}, I) \cup Sol(C(ML_{ji}, AL_{ji}, I)$.

- Si $ML_{ij}u \in Sol(C(ML_{ij}, AL_{ij}, I))$, le vecteur u vérifie $AL_{ij}u = 0$ et $\forall k \in I$, $u_k = 0$.
  Posons $v = L_{ij}u$. On a $v_k = u_k$ si $k \neq i$ et $v_i = u_i + u_j$.
  Ainsi, $v \in \mathbb{N}^k$, $\forall k \in I$, $v_k = 0$ (car $i \notin I$) et $Av = AL_{ij}u = 0$ donc $Mv \in Sol(C(M,A,I))$, ce qui prouve que $Sol(C(ML_{ij}, AL_{ij}, I)) \subset Sol(C(M,A,I))$. De même, $Sol(C(ML_{ji}, AL_{ji}, I)) \subset Sol(C(M,A,I))$.
- Réciproquement, si $Mu \in Sol(C(M,A,I))$, on a $Au = 0$ et $\forall k \in I$, $u_k = 0$.
  Si $u_i \geqslant u_j$, posons $v = L_{ij}^{-1}u$. On a $v_k = u_k$ si $k \neq i$ et $v_i = u_i - u_j$.
  Ainsi, $v \in \mathbb{N}^k$, $\forall k \in I$, $v_k = 0$ et $AL_{ij}v = Au = 0$ donc $ML_{ij}v = Mu \in Sol(ML_{ij}, AL_{ij}, I)$.
  De même, si $u_j \geqslant u_i$ on prouve que $Mu \in Sol(ML_{ji}, AL_{ji}, I)$.

– Si les A_{1i}, $i \notin I$ sont tous de même signe, nous allons montrer que $Sol(C(M,A,I)) = Sol(C(M,A',I'))$.

- Si $Mu \in Sol(C(M,A,I))$, on a $Au = 0$ et $\forall i \in I$, $u_i = 0$.
  Mais alors $A_{1*}u = 0$ et $A'u = 0$. La première condition garantit que $\forall i \in I'$, $u_i = 0$ (une somme de termes positifs ne peut être nulle que si chacun des termes l'est), donc $Mu \in Sol(C(M,A',I'))$.
- Réciproquement, si $Mu \in Sol(C(M,A',I'))$, on a $A'u = 0$ et $\forall i \in I'$, $u_i = 0$. Alors $A_{1*}u = 0$ donc $Au = 0$, et $Mu \in Sol(C(M,A,I))$.

Ainsi, si $E' =$ `transf`(E) on a toujours $Sol(E) = Sol(E')$.

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

On applique l'algorithme `Transf` sur le singleton $\{C(Id,A,\emptyset)\}$. On obtient un ensemble de contraintes sous formes résolues $C(M_i, \varepsilon, I_i)$, $1 \leqslant i \leqslant n$.
Notons (e) la base canonique $\mathbb{R}^k$. Alors l'ensemble des vecteurs de la forme $M_i e_j$ avec $j \notin I_i$ constitue une base de S(A). D'après la question 2.4 il suffit pour obtenir H(A) de ne garder que les solutions minimales de cet ensemble de vecteurs.

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.*
Calculer ML_{ij} revient à ajouter la colonne i à la colonne j. On peut donc s'inspirer de la représentation de la méthode du pivot pour appliquer l'algorithme, en représentant la contrainte C(M, A, I) par une matrice $\begin{bmatrix} M \\ A \end{bmatrix}$ dans laquelle les colonnes d'indice $i \in I$ sont supprimées car non utiles pour la suite. Il s'agit alors d'appliquer `Transf` à la contrainte $C(Id, A, \emptyset)$.

Étape 1 : la première ligne de A possède des coefficients de signes opposés dans les colonnes 2 et 4 ; il faut donc effectuer les opérations élémentaires $C_4 \leftarrow C_4 + C_2$ et $C_2 \leftarrow C_2 + C_4$ sur deux copies de A et M. On obtient :

$$\left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \hline 0 & -1 & 0 & 0 \\ 1 & 0 & 1 & -3 \end{array}\right] \quad \text{et} \quad \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 1 \\ 1 & -3 & 1 & -3 \end{array}\right]$$

Étape 2 : dans les deux cas, la matrice A ne possède plus de termes de signes contraires dans sa première ligne. On supprime cette ligne ainsi que les colonnes dont les coefficients de la première ligne sont non nuls (la deuxième colonne à gauche et la quatrième à droite).

$$\left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 1 & -3 \end{array}\right] \quad \text{et} \quad \left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ \hline 1 & -3 & 1 \end{array}\right]$$

On poursuit ainsi en appliquant l'étape 1 jusqu'à ne plus obtenir de termes de signes opposés sur la première (et maintenant unique) ligne de A. Quand l'étape 2 s'applique enfin on a alors $A = \varepsilon$ et dans ce cas les colonnes restantes de M forment des éléments d'une base de S(A).

Cependant, même ainsi le nombre de matrices à gérer augmente assez vite et rend ce travail fastidieux. Après plusieurs tentatives, j'ai fini par me dire qu'il serait plus confortable de programmer effectivement cet algorithme en Python (c'est après tout à cela que sert un algorithme). Une fois ceci fait [1], j'ai obtenu 30 vecteurs (ce qui montre qu'à la main ce calcul doit être vraiment fastidieux …), mais seulement 4 distincts :

$$\begin{pmatrix} 1 \\ 1 \\ 2 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 3 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 1 \\ 0 \\ 1 \end{pmatrix}$$

Ces vecteurs constituent une base de S(A) ; ceux qui sont minimaux sont les éléments de H(A).
Il reste à observer que si X est une solution non minimale et non nulle, il existe $Y \in S(A)$ tel que $Y < X$. Puisque Y est combinaison linéaire à coefficients positifs d'une base de S(A), au moins un vecteur V de la base va lui aussi vérifier $V < X$. Or il n'existe aucune relation d'ordre entre les quatre vecteurs ci-dessus ; on peut donc affirmer qu'ils sont tous quatre minimaux et que H(A) est l'ensemble de ces quatre vecteurs.

Partie 3. Problème de Frobenius

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

Il est bien évident que la condition (i) implique la condition (ii), mais la réciproque est fausse : $\text{pgcd}(2,3) = 1$ mais pourtant l'équation $2x_1 + 3x_2 = 1$ ne possède pas de solution dans $\mathbb{N}^2$.

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).*

Si $\text{pgcd}(a_1,\dots,a_n) = 1$, il existe des entiers relatifs $x_1,\dots,x_n$ vérifiant : $a_1x_1 + \cdots + a_nx_n = 1$. Notons que l'un au moins des x_i doit être strictement négatif puisque les a_i sont supérieurs ou égaux à 2.
Sans perte de généralité on peut supposer $x_1,\dots,x_i$ positifs ou nuls et $x_{i+1},\dots,x_n$ strictement négatifs. En posant $K = -a_{i+1}x_{i+1} \cdots - a_nx_n$ on a $1 + K = a_1x_1 + \cdots + a_ix_i$, et K et $1 + K$ sont tous deux des combinaisons linéaires positives des a_i. Posons alors $N = K^2$. Pour tout $b \geqslant N$ on a $b = qK + r$ avec $q \geqslant K$ et $0 \leqslant r < K$. Alors :

$$b = qK + r = qK + r(K + 1 - K) = (q - r)K + r(K + 1)$$

et b est bien combinaison linéaire positive des a_i.

1. Le script que j'ai utilisé figure en annexe.

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

(a) Supposons que $ab-a-b \in \mathrm{T}$: il existe x_1 et x_2 positifs tels que $ab-a-b = ax_1+bx_2$. On a donc $a(b-1-x_1) = b(1+x_2)$. Le terme de droite est strictement positif donc $0 < b-1-x_1 < b$. Mais a et b sont premiers entre eux donc b doit diviser $b-1-x_1$, ce qui ne se peut.

(b) Soit $(u,v) \in \mathbb{Z}^2$ tel que $au+bv = 1$. Alors $k = a(ku)+b(kv)$. Effectuons la division euclidienne de kv par a : $kv = qa+r$ avec $0 \leqslant r < a$. Alors $k = a(ku+qb)+br$ avec $ku+qb \in \mathbb{Z}$ et $0 \leqslant r < a$.

(c) D'après (b) il existe $v_1 \in \mathbb{Z}$ et $v_2 \in \mathbb{N}$ tel que $ab-a-b+i = v_1a+v_2b$ avec $v_2 \leqslant a-1$.
Alors $(1+v_1)a = ab-b+i-v_2b = i+(a-1-v_2)b \geqslant i > 0$, ce qui implique $v_1 \geqslant 0$.

(d) De (a) et (c) on déduit immédiatement que $g(a,b) = ab-a-b$.

Question 3.4 *Cette question ainsi que les suivantes ont été très peu abordées.*

Soit $\ell \in [\![0, a_n-1]\!]$, et $k \in [\![1,n]\!]$ tel que l'entier $x = g(a_1,\dots,a_n)+k$ vérifie $x \equiv \ell \bmod a_n$.
On a $x > g(a_1,\dots,a_n)$ donc x est combinaison linéaire positive des a_i : $x = a_1x_1+\cdots+a_nx_n$ avec $x_i \geqslant 0$.
On a $a_1x_1+\cdots+a_{n-1}x_{n-1} \equiv \ell \bmod a_n$ donc par définition de t_ℓ on a $t_\ell \leqslant a_1x_1+\cdots+a_{n-1}x_{n-1} \leqslant x = g(a_1,\dots,a_n)+k$.
Ceci prouve que $\max\limits_{\ell} t_\ell \leqslant g(a_1,\dots,a_n)+a_n$.
Réciproquement, posons $g(a_1,\dots,a_n)+a_n = a_1y_1+\cdots+a_ny_n$ avec $y_i \geqslant 0$. On a nécessairement $y_n = 0$ car sinon $g(a_1,\dots,a_n)$ serait combinaison linéaire positive des a_i. Ainsi, $g(a_1,\dots,a_n)+a_n = a_1y_1+\cdots+a_{n-1}y_{n-1}$.
Soit $\ell \in [\![0,a_n-1]\!]$ tel que $g(a_1,\dots,a_n)+a_n \equiv \ell \bmod a_n$. Alors $g(a_1,\dots,a_n)+a_n = t_\ell+qa_n$ avec $q \geqslant 0$. Mais si on avait $q \geqslant 1$, $g(a_1,\dots,a_n)$ serait combinaison linéaire positive des a_i, ce qui est absurde. On a donc $t_\ell = g(a_1,\dots,a_n)+a_n$, ce qui achève de prouver l'inégalité demandée.

Question 3.5 Soit $x = (x_1,\dots,x_{n-1}) \in \mathbb{Z}^{n-1}$, et ℓ le reste de la division euclidienne de $a_1x_1+\cdots+a_{n-1}x_{n-1}$ par a_n. Posons $t_\ell = a_1y_1+\cdots+a_{n-1}y_{n-1}$, avec $y_i \geqslant 0$, et $y = (y_1,\dots,y_{n-1})$.
On a $a_1x_1+\cdots+a_{n-1}x_{n-1} \equiv \ell \bmod a_n \equiv a_1y_1+\cdots+a_{n-1}y_{n-1}$ donc $x-y \in \mathrm{L}$.
Par ailleurs, $t_\ell \leqslant g(a_1,\dots,a_n)+a_n$ (question 3.4) donc il existe $\lambda \in [0,1]$ tel que $a_1y_1+\cdots+a_{n-1}y_{n-1} = \lambda(g(a_1,\dots,a_n)+a_n)$, et ainsi $y \in (g(a_1,\dots,a_n)+a_n)\mathrm{S}$. On a donc $x = y+(x-y) \in (g(a_1,\dots,a_n)+a_n)\mathrm{S}+\mathrm{L}$.

Question 3.6 Soit $x = (x_1,\dots,x_{n-1}) \in \mathbb{R}^{n-1}$. On a $x = (\lfloor x_1 \rfloor,\dots,\lfloor x_{n-1} \rfloor)+(y_1,\dots,y_{n-1})$ avec $y_i \in [0,1[$ donc

$$\mathbb{R}^{n-1} \subset \mathbb{Z}^{n-1}+(a_1+\cdots+a_{n-1})\mathrm{S}.$$

D'après la question précédente on en déduit : $\mathbb{R}^{n-1} \subset (g(a_1,\dots,a_n)+a_1+\cdots+a_n)\mathrm{S}+\mathrm{L}$, ce qui prouve que $\mu(\mathrm{S},\mathrm{L})$ existe et $\mu(\mathrm{S},\mathrm{L}) \leqslant g(a_1,\dots,a_n)+a_1+\cdots+a_n$.

Question 3.7 Considérons un réel t tel que $\mathbb{Z}^{n-1} \subset t\mathrm{S}+\mathrm{L}$.
Soit $\ell \in [\![0,a_n-1]\!]$, et $x \in \mathbb{Z}^{n-1}$ tel que $a_1x_1+\cdots+a_{n-1}x_{n-1} \equiv \ell \bmod a_n$. On a $x \in t\mathrm{S}+\mathrm{L}$ donc on peut écrire : $x = ty+z$ avec $y \in \mathrm{S}$ et $z \in \mathrm{L}$.
$ty = x-z \in \mathbb{N}^{n-1}$ et $t(a_1y_1+\cdots+a_ny_n) \equiv \ell \bmod a_n$ donc $t_\ell \leqslant t(a_1y_1+\cdots+a_ny_n)$ (par définition de t_ℓ). Et puisque $y \in \mathrm{S}$ il en résulte que $t_\ell \leqslant t$. Ceci étant vrai pour tout ℓ on en déduit que $g(a_1,\dots,a_n)+a_n \leqslant t$. On conclut avec la question 3.5.

Question 3.8 Compte tenu de la question3.6 il reste à prouver que $\mu(s,\mathrm{L}) \geqslant g(a_1,\dots,a_n)+a_1+\cdots+a_n$.
Considérons un réel $t < g(a_1,\dots,a_n)+a_n$. D'après la question précédente, $t\mathrm{S}+\mathrm{L}$ ne contient pas $\mathbb{Z}^{n-1}$ donc il existe $y \in \mathbb{Z}^{n-1}$ tel que pour tout $x \in \mathrm{L}$ on ait $y-x \notin t\mathrm{S}$.
En particulier, pour tout $x \in \mathrm{L}$ tel que $y_i-x_i \geqslant 0$ on a $a_1(y_1-x_1)+\cdots+a_{n-1}(y_{n-1}-x_{n-1}) > t$.
Soit alors $\varepsilon \in]0,1[$ et $z \in \mathbb{R}^{n-1}$ défini par $z_i = y_i+\varepsilon$.
Quel que soit $x \in \mathrm{L}$ vérifiant $z_i \geqslant x_i$ on a aussi $y_i \geqslant x_i$ (il s'agit d'entiers, et $\varepsilon < 1$) donc :

$$a_1(z_1-x_1)+\cdots+a_{n-1}(z_{n-1}-x_{n-1}) > \varepsilon(a_1+\cdots+a_{n-1})+t.$$

Ainsi, $z \notin (t+\varepsilon(a_1+\cdots+a_{n-1}))\mathrm{S}+\mathrm{L}$, ce qui prouve que $t+\varepsilon(a_1+\cdots+a_{n-1}) < \mu(\mathrm{S},\mathrm{L})$.
En faisant tendre ε vers 1 on obtient : $\mu(\mathrm{S},\mathrm{L}) \geqslant t+a_1+\cdots+a_{n-1}$, et puisque t peut être rendu aussi proche que l'on veut de $g(a_1,\dots,a_n)+a_n$ on peut conclure :

$$\mu(\mathrm{S},\mathrm{L}) \geqslant g(a_1,\dots,a_n)+a_1+\cdots+a_n.$$

Partie 4. Dénumérants et borne inférieure sur le nombre de Frobenius

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.*

La fonction $x \mapsto \dfrac{1}{1-x}$ est développable en série entière sur $]-1,1[$ donc il en est de même de f, et pour tout $x \in]-1,1[$,

$$f(x) = \Big(\sum_{k=0}^{+\infty} x^{a_1 k}\Big)\cdots\Big(\sum_{k=0}^{+\infty} x^{a_n k}\Big) = \sum_{k_1,\dots,k_n \geqslant 0} x^{a_1k_1+\cdots+a_nk_n} = \sum_{i=0}^{+\infty} d(i,a_1,\dots,a_n)x^i.$$

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.*

Il suffit de développer en série entière $f(x) = \dfrac{1}{(1-x)(1-x^2)} = \dfrac{1}{4}\Big(\dfrac{1}{1+x} + \dfrac{1}{1-x} + \dfrac{2}{(1-x)^2}\Big)$:

$$f(x) = \frac{1}{4}\sum_{n=0}^{+\infty}\Big((-1)^n x^n + x^n\Big) + \frac{1}{2}\sum_{n=0}^{+\infty}(n+1)x^n = \frac{1}{4}\sum_{n=0}^{+\infty}\Big((-1)^n + 1 + 2(n+1)\Big)x^n.$$

On en déduit que $d(m,1,2) = \dfrac{1}{4}\Big(2m+3+(-1)^m\Big)$.

Question 4.3 Soit $x \in \mathrm{P}(m)$. Pour tout $i \in [\![1,n]\!]$ on pose $b_i = \left\lfloor \dfrac{x_i}{a_i} \right\rfloor$. Alors $x \in \mathrm{B}(b_1,\dots,b_n)$ et $a_1b_1+\cdots+a_nb_n \leqslant x_1+\cdots+x_n \leqslant m$, d'où l'inclusion demandée.

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

Le « volume » de $\mathrm{B}(b_1,\dots,b_n)$ est égal à p_n et celui de $\mathrm{P}(m)$ à $\dfrac{m^n}{n!}$ (ce dernier point se montre par récurrence). D'après la question précédente on a donc : $\dfrac{m^n}{n!} \leqslant d'(m,a_1,\dots,a_n)p_n$.

Pour prouver l'autre inégalité, considérons $(b_1,\dots,b_n)$ tel que $b_1a_1+\cdots+b_na_n \leqslant m$, et $x \in \mathrm{B}(b_1,\dots,b_n)$.

$x_1+\cdots+x_n \leqslant (b_1+1)a_1+\cdots+(b_n+1)a_n \leqslant m+s_n$ donc $x \in \mathrm{P}(m+s_n)$. On a donc $\displaystyle\bigcup_{b_1a_1+\cdots+b_na_n\leqslant m} \mathrm{B}(b_1,\dots,b_n) \subset \mathrm{P}(m+s_n)$.

Sachant que cette union est disjointe, le passage aux volumes conduit à l'inégalité : $d'(m,a_1,\dots,a_n)p_n \leqslant \dfrac{(m+s_n)^n}{n!}$.

On a donc bien $\dfrac{m^n}{n!p_n} \leqslant d'(m,a_1,\dots,a_n) \leqslant \dfrac{(m+s_n)^n}{n!p_n}$.

Question 4.5 *La fin du problème n'a pas été abordée, du moins avec succès.*

Soit $y > 0$ et M le nombre de solutions de l'inégalité $a_1x_1+\cdots+a_nx_n \leqslant g_n+y$.

D'après la question précédente, $\mathrm{M} \leqslant \dfrac{(g_n+y+s_n)^n}{n!p_n}$.

Par ailleurs, pour tout entier $k \in [\![1,\lfloor y \rfloor]\!]$ et par définition de g_n, il existe $x_1,\dots,x_n$ dans $\mathbb{N}^n$ tel que $a_1x_1+\cdots+a_nx_n = g_n+k$. Ceci nous donne déjà $\lfloor y \rfloor$ solutions distinctes de l'inégalité $a_1x_1+\cdots+a_nx_n \leqslant g_n+y$.

$(0,\dots,0)$ est aussi solution, donc on peut affirmer que $\mathrm{M} \geqslant \lfloor y \rfloor + 1 > y$ et ainsi, $y < \dfrac{(g_n+y+s_n)^n}{n!p_n}$, ce qui montre que $f(y) > n!p_n$.

Question 4.6 Une étude immédiate de la fonction f montre que celle-ci est minimale pour $y_0 = \dfrac{g_n+s_n}{n-1}$, ce qui conduit à l'inégalité : $f(y_0) = \dfrac{n^n(g_n+s_n)^{n-1}}{(n-1)^{n-1}} > n!p_n$ puis $g_n > \dfrac{n-1}{n}\Big((n-1)!p_n\Big)^{\frac{1}{n-1}} - s_n$.

Le script utilisé à la question 2.12

```
import numpy as np


def deMemeSigne(A):
    x = y = 0
    for a in A[0]:
        if a > 0:
            x += 1
        elif a < 0:
            y += 1
    return x == 0 or y == 0


def mini(A):
    i = j = None
    for k, a in enumerate(A[0]):
        if a > 0:
            if i is None or a > A[0, i]:
                i = k
        elif a < 0:
            if j is None or a < A[0, j]:
                j = k
    return i, j


def transf(M, A, sol):
    n, p = A.shape
    if n == 0:
        for j in range(p):
            sol.append(M[:, j])
    elif not deMemeSigne(A):
        i, j = mini(A)
        M1 = M.copy()
        A1 = A.copy()
        M1[:, i] += M1[:, j]
        A1[:, i] += A1[:, j]
        transf(M1, A1, sol)
        M[:, j] += M[:, i]
        A[:, j] += A[:, i]
        transf(M, A, sol)
    else:
        l = []
        for j, a in enumerate(A[0]):
            if a != 0:
                l.append(j)
        M = np.delete(M, l, axis=1)
        A = np.delete(np.delete(A, l, axis=1), 0, axis=0)
        transf(M, A, sol)


A = np.array([[0, -1, 0, 1], [1, 0, 1, -3]])
M = np.diag([1, 1, 1, 1])
sol = []
transf(M, A, sol)
```