Corrigé de l'épreuve de Mathématiques-Informatique 2002
ENS Ulm et Lyon

Alain Darte* Jean Mairesse†

Autour des carrés latins

Partie 1. Quelques propriétés des matrices carrées entières

Question 1.1.

Par simple calcul matriciel, on obtient :

$$(AE_{i,j})(k,l) = \sum_p A(k,p)E_{i,j}(p,l) = A(k,i)E_{i,j}(i,l) \text{ puisque } E_{i,j}(p,l) = 0 \text{ si } p \neq i\,.$$

On a alors, pour tout k, $(AE_{i,j})(k,j) = A(k,i)$ et $(AE_{i,j})(k,l) = 0$ si $l \neq j$. La matrice $AE_{i,j}$ est donc la matrice dont tous les coefficients sont nuls sauf la colonne j qui vaut la colonne i de la matrice A. On vérifie alors aisément que $AP_{i,j} = A - AE_{i,i} - AE_{j,j} + AE_{i,j} + AE_{j,i}$ est la matrice obtenue à partir de A en échangeant les colonnes i et j, que $AS_i = A - 2AE_{i,i}$ est celle obtenue en transformant la colonne i en son opposé et que $AR_{i,j} = A - AE_{i,j}$ est celle obtenue en retranchant la colonne i à la colonne j (terme à terme).

Les matrices S_i sont diagonales et on a $\det(S_i) = -1$; les matrices $R_{i,j}$ sont triangulaires et on a $\det(R_{i,j}) = 1$. Lorsque $i = j$, on a $P_{i,j} = I$ et le déterminant vaut 1. Lorsque $i \neq j$, la matrice obtenue en permutant les colonnes i et j de $P_{i,j}$ est la matrice identité. Donc, le déterminant de $P_{i,j}$ vaut -1 (signature d'une transposition).

On trouve (sans aucun calcul) l'inverse d'une matrice élémentaire à partir de l'interprétation de l'effet du produit à droite par cette matrice :

$$P_{i,j}P_{i,j} = I,\ S_iS_i = I,\ R_{i,j}(I + E_{i,j}) = (I + E_{i,j})R_{i,j} = I\,.$$

Enfin, on constate que $I + E_{i,j} = S_iR_{i,j}S_i$ puisque pour ajouter la colonne i à la colonne j, il suffit de changer le signe de la colonne i, de la soustraire à la colonne j, puis de changer à nouveau le signe de la colonne i. L'inverse de $R_{i,j}$ est donc un produit de matrices élémentaires.

Question 1.2.

Les différentes opérations effectuées sur la matrice A consistent toutes à multiplier à droite par une des matrices élémentaires. On remarque également que multiplier à droite par $(R_{i,j})^q$ revient à soustraire q fois la colonne i à la colonne j.

*LIP, CNRS - ENS-Lyon, 46, Allée d'Italie, 69364 Lyon Cedex 07;
†LIAFA, CNRS - Université Paris 7, Case 7014 - 2, place Jussieu, 75251 Paris Cedex 05.

Si tous les coefficients de la ligne d'indice 0 de A sont nuls, la matrice A est inchangée (on a $C = \emptyset$ en entrée de la boucle **Tant que** et l'algorithme se termine). Dans le cas contraire, après la première opération (première boucle **Pour**), tous les coefficients de la ligne 0 de A deviennent positifs ou nuls. La seconde opération (début de la boucle **Tant que**) a pour effet de se ramener à une matrice dont le coefficient d'indice $(0, 0)$ est le plus petit coefficient non nul de la ligne 0. La troisième opération (seconde boucle **Pour**) a pour effet de soustraire un nombre entier et maximal de fois la colonne 0 aux autres colonnes, la contrainte étant de conserver une ligne 0 à coefficients positifs ou nuls : q est le quotient de la division euclidienne de $A(0, k)$ par $A(0, 0)$, et le nouveau coefficient après cette étape est donc le reste de la division euclidienne de $A(0, k)$ par $A(0, 0)$. On se retrouve alors avec une ligne 0 possédant un unique coefficient maximal qui est celui d'indice $(0, 0)$.

À chaque passage dans la boucle **Tant que**, la somme des coefficients de la ligne 0 diminue strictement (et le coefficient placé en position $(0, 0)$ également). Ces nombres étant strictement positifs et entiers, on en déduit que l'algorithme se termine. Ainsi, la répétition des opérations 2 et 3 (sélection du plus petit coefficient non nul, puis pas élémentaire de l'algorithme d'Euclide) conduit à ce qu'il n'y ait plus que le coefficient d'indice $(0, 0)$ qui soit non nul en ligne 0.

Sur chacune des lignes, les opérations effectuées consistent à changer le signe d'un coefficient, à permuter deux coefficients, ou à ajouter un multiple d'un coefficient à un autre. Les deux premières opérations ne changent évidemment pas le pgcd. Pour la troisième, il suffit de vérifier que pour deux entiers a_1 et b_1, et un entier q, on a $a_1 \wedge a_2 = a_1 \wedge (a_2 - qa_1)$, ce qui est immédiat. Cette propriété s'étend pour le pgcd des coefficients de toute une ligne :

$$a_1 \wedge \ldots \wedge a_i \wedge \ldots \wedge a_{n-1} = a_1 \wedge \ldots \wedge (a_i - qa_1) \wedge \ldots \wedge a_{n-1} \, .$$

Le pgcd de chacune des lignes est donc inchangé par l'algorithme puisque chacune des opérations élémentaires le laisse inchangé.

On peut aussi raisonner avec la propriété de Bezout. Notons B la matrice obtenue après application de l'algorithme. Il existe Q (produit de matrices élémentaires) telle que $B = AQ$. Soit $i \in \mathcal{N}_n$ et p_i le pgcd des coefficients $(B(i,j))_{j \in \mathcal{N}_n}$. Il existe des entiers $(u_{i,j})_{j \in \mathcal{N}_n}$ (coefficients de Bezout) tels que $p_i = \sum_j B(i,j) u_{i,j}$. Puisque $B(i,j) = \sum_k A(i,k) Q(k,j)$, on a $p_i = \sum_j (\sum_k A(i,k) Q(k,j)) u_{i,j} = \sum_k A(i,k) (\sum_j Q(k,j) u_{i,j}) = \sum_k A(i,k) v_{i,k}$. Ainsi, p_i est un multiple du pgcd des coefficients de la ligne i de la matrice A. Réciproquement, puisque Q a un inverse dans $\mathcal{M}_n(\mathbb{Z})$ (comme produit de matrices dont on a montré qu'elles étaient inversibles dans $\mathcal{M}_n(\mathbb{Z})$), on peut faire le même raisonnement pour $A = BQ^{-1}$ et montrer ainsi que les deux pgcd sont égaux.

Remarque Dans de nombreuses copies, on trouve l'argument (faux) suivant : l'algorithme termine car $\mathrm{Card}(C)$ décroit strictement à chaque itération de la boucle **Tant que**.

Question 1.3.

L'algorithme de la question précédente permettait de rendre nulle la ligne d'indice 0 de la matrice A sauf éventuellement le coefficient d'indice $(0, 0)$. Il suffit d'appliquer le même principe à la sous-matrice, de taille $(n-1)$, inférieure droite en considérant les $(n-1)$ dernières lignes et en n'effectuant que des opérations sur les $(n-1)$ dernières colonnes. Ainsi, on ne modifiera pas la colonne 0 de A et les $(n-1)$ derniers coefficients de la ligne d'indice 0 étant nuls, ils le resteront. Il suffit d'ajouter une boucle **Pour** extérieure, pour parcourir les indices de lignes, et de modifier légèrement les indices dans l'algorithme de la question 1.2 de manière adéquate. Enfin, si on effectue les opérations sur une copie H de A, on obtiendra en sortie $H = AQ_1Q_2\cdots$ où H est triangulaire inférieure à diagonale positive ou nulle et les Q_i sont les matrices élémentaires successives utilisées dans l'algorithme. On a donc $A = HQ$ avec $Q = \cdots Q_2^{-1}Q_1^{-1}$. Comme on a montré à la question 1.1 que l'inverse d'une matrice élémentaire peut s'écrire comme un produit de matrices élémentaires, on a le résultat voulu. Pour obtenir directement la matrice Q, il faut mémoriser les produits à gauche des inverses des matrices élémentaires utilisées, ce qui conduit à l'algorithme de la figure 1.

H = A ; Q = I ;
Pour i **de** 0 **à** $n-1$
    Pour j **de** i **à** $n-1$
        Si $(H(i,j) < 0)$
            $H \leftarrow HS_j$;
            $Q \leftarrow S_jQ$;
        FinSi
    FinPour
    $C \leftarrow \{j \in \mathcal{N}_n \setminus \mathcal{N}_{i-1} \mid H(i,j) \neq 0\}$;
    Tant que $(C \neq \emptyset)$
        $m \leftarrow \min\{H(i,j) \mid j \in C\}$;
        Soit $k \in C$ tel que $H(i,k) = m$;
        $H \leftarrow HP_{i,k}$;
        $Q \leftarrow P_{i,k}\,Q$
        Pour j **de** $i+1$ **à** $n-1$
            $q \leftarrow H(i,j) \div m$;
            $H \leftarrow H(R_{i,j})^q$;
            $Q \leftarrow (I + qE_{i,j})\,Q$;
        FinPour
        $C \leftarrow \{j \in \mathcal{N}_n \setminus \mathcal{N}_i \mid H(i,j) \neq 0\}$;
    FinTantQue
FinPour

FIG. 1 – Algorithme de la question 1.2.

Pour i **de** 0 **à** $n-1$
    Pour j **de** 0 **à** $i-1$
        $q \leftarrow H(i,j) \div H(i,i)$;
        $H \leftarrow H(R_{i,j})^q$;
        $Q \leftarrow (I + qE_{i,j})\,Q$;
    FinPour
FinPour

FIG. 2 – Étape supplémentaire.

La matrice Q est un produit fini de matrices élémentaires, toutes de déterminant 1 ou -1, et inversibles dans $\mathcal{M}_n(\mathbb{Z})$, d'après la question 1.1. La matrice Q est donc inversible dans $\mathcal{M}_n(\mathbb{Z})$ et de déterminant 1 ou -1, c'est-à-dire unimodulaire.

Si $\det(A) \neq 0$, alors $\det(H) \neq 0$ et tous les termes diagonaux de H sont strictement positifs. Pour chaque indice i, on peut alors ajouter ou soustraire la colonne i suffisamment de fois aux colonnes précédentes pour que tous les coefficients de la ligne i soient positifs et strictement plus petits que l'élément diagonal de cette ligne. Ceci ne modifiera pas (du fait de la forme triangulaire de H) les coefficients des lignes précédentes, ni la forme triangulaire de la matrice. En revanche, il faut faire attention à effectuer ces opérations dans l'ordre des i croissants. Pour cela, il suffit de remplacer, dans l'algorithme de la figure 1, la boucle sur

j (celle de $i+1$ à $n-1$) par une boucle pour tout $j \in \mathcal{N}_n$, $j \neq i$. En termes d'opérations effectuées, mieux vaut néanmoins effectuer cette opération supplémentaire en fin d'algorithme, une fois que H est déjà triangulaire. On rajoute alors le code de la figure 2.

Remarque L'algorithme proposé est une adaptation de l'algorithme du pivot de Gauss au cas des matrices entières.

Question 1.4.

Soit A une matrice unimodulaire, vérifiant donc $|\det(A)| = 1$. Il existe une décomposition sous la forme $A = HQ$ où H et Q vérifient toutes les conditions de la question précédente. On a $\det(A) = \det(H)\det(Q)$ et $|\det(A)| = |\det(Q)| = 1$. On en déduit que $|\det(H)| = 1$. Comme H est triangulaire, on a $\det(H) = \prod_i H(i,i)$ et, puisque $H(i,i) \in \mathbb{N}^*$ pour tout i, $H(i,i) = 1$ pour tout i. Enfin, comme $0 \leq H(j,i) < H(i,i)$ pour tout $j < i$, on conclut que H est la matrice identité. On a donc $A = Q$ et A est produit de matrices élémentaires.

D'après la question 1.1, les matrices élémentaires sont inversibles dans $\mathcal{M}_n(\mathbb{Z})$, donc toute matrice unimodulaire est inversible dans $\mathcal{M}_n(\mathbb{Z})$ comme produit de matrices élémentaires. Réciproquement, soit A une matrice inversible de $\mathcal{M}_n(\mathbb{Z})$, c'est-à-dire telle que $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$. On a $\det(A) \in \mathbb{Z}$ et $\det(A^{-1}) \in \mathbb{Z}$ puisque le déterminant est un polynôme en les coefficients de la matrice :

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) \prod_{i=0}^{n-1} A(i, \sigma(i)) \ . \tag{1}$$

Enfin, puisque $\det(A)\det(A^{-1}) = 1$, on en conclut que $\det(A) = \det(A^{-1}) = 1$ ou $\det(A) = \det(A^{-1}) = -1$. En particulier, A est unimodulaire.

Remarque Il n'est pas nécessaire d'utiliser la première partie de la question pour montrer qu'une matrice unimodulaire est inversible dans $\mathcal{M}_n(\mathbb{Z})$. Voici une preuve plus directe. Soit A une matrice unimodulaire. On a :

$$\tilde{A}^T A = A \tilde{A}^T = \det(A) I \ ,$$

avec $\tilde{A}$ la matrice des cofacteurs définie par $\tilde{A}(i,j) = (-1)^{i+j}\det(A_{[i,j]})$, où $A_{[i,j]}$ est la matrice obtenue à partir de A en supprimant la ligne i et la colonne j. Comme les matrices $A_{[i,j]}$ sont à coefficients entiers, $\tilde{A}$ est aussi à coefficients entiers. Enfin comme $|\det(A)| = 1$, $\det(A)$ est inversible dans $\mathbb{Z}$ et $\det(A)^{-1}\tilde{A}^T$, à coefficients entiers, est l'inverse de A.

Question 1.5.

Soit $A \in \mathcal{M}_n(\mathbb{Z})$ avec $\det(A) \neq 0$. Supposons que $A = H_1 Q_1 = H_2 Q_2$ où (H_1, Q_1) et (H_2, Q_2) vérifient toutes les conditions de la question 1.3. On a $H_1 = H_2 Q$ avec $Q = Q_2 Q_1^{-1}$. On sait que l'inverse d'une matrice triangulaire inférieure est triangulaire inférieure. On en déduit que $Q = H_1 H_2^{-1}$ est triangulaire inférieure. Comme par ailleurs Q est unimodulaire, on en déduit que tous ses coefficients diagonaux sont égaux à 1 ou -1.

Puisque H_1, H_2 et Q sont toutes trois triangulaires inférieures, on peut calculer simplement la diagonale de H_1 : pour tout i, $H_1(i,i) = H_2(i,i)Q(i,i)$. Or $H_1(i,i)$ et $H_2(i,i)$ sont tous deux strictement positifs, donc $Q(i,i)$ est strictement positif pour tout i, donc égal à 1. Ceci implique que H_1 et H_2 coïncident sur la diagonale principale. Montrons le même résultat pour la première sous-diagonale. Pour tout $i > 0$, on a :

$$H_1(i,i-1) = H_2(i,i-1)Q(i-1,i-1) + H_2(i,i)Q(i,i-1) = H_2(i,i-1) + H_2(i,i)Q(i,i-1)\,.$$

Or, par définition, $0 \leq H_1(i,i-1) < H_1(i,i)$ et $0 \leq H_2(i,i-1) < H_2(i,i) = H_1(i,i)$. On en déduit que $Q(i,i-1) = 0$ et donc que $H_1(i,i-1) = H_2(i,i-1)$. Les premières sous-diagonales de H_1 et H_2 sont donc identiques et de plus, la première sous-diagonale de Q est nulle.

On raisonne maintenant par récurrence. Supposons que les $(k-1)$ premières sous-diagonales de H_1 et H_2 sont identiques et que les $(k-1)$ premières sous-diagonales de Q sont nulles. On a :

$$\begin{aligned} H_1(i,i-k) &= \sum_{j=0}^{n} H_2(i,j)Q(j,i-k) \\ &= \sum_{j=i-k}^{i} H_2(i,j)Q(j,i-k) \\ &= H_2(i,i-k)Q(i-k,i-k) + H_2(i,i)Q(i,i-k) \\ &= H_2(i,i-k) + H_2(i,i)Q(i,i-k)\,. \end{aligned}$$

On en déduit alors comme précédemment que $Q(i,i-k) = 0$ pour tout i, c'est-à-dire que la k-ième sous-diagonale de Q est nulle, puis que les k-ièmes sous-diagonales de H_2 et H_1 sont identiques.

Question 1.6.

Supposons que $\vec{0}$ soit l'unique solution entière de $A\vec{x} \bmod \vec{a} = \vec{0}$ avec $\forall i, -c_i < x_i < c_i$. Soient $\vec{y}$ et $\vec{z}$ dans $\mathcal{N}_{\vec{c}}$ tels que $A\vec{y} \bmod \vec{a} = A\vec{z} \bmod \vec{a}$. On a alors $A(\vec{y}-\vec{z}) \bmod \vec{a} = \vec{0}$ et $\forall i, -c_i < y_i - z_i < c_i$. On en déduit $\vec{y} = \vec{z}$ et l'injectivité souhaitée.

Réciproquement, soit $\vec{x}$ tel que $A\vec{x} \bmod \vec{a} = \vec{0}$. Définissons $\vec{y}$ et $\vec{z}$ tels que :

$$y_i = \max(x_i, 0), \quad z_i = -\min(x_i, 0)\,.$$

Alors, $\vec{y} \in \mathcal{N}_{\vec{c}}$, $\vec{z} \in \mathcal{N}_{\vec{c}}$ et $\vec{y} - \vec{z} = \vec{x}$. Puisque $\vec{y}$ et $\vec{z}$ ont la même image par $A_{\vec{a}}$, l'injectivité de $A_{\vec{a}}$ sur $\mathcal{N}_{\vec{c}}$ implique $\vec{y} = \vec{z}$, puis finalement $\vec{x} = \vec{0}$.

Remarque Il est frappant de constater que seuls 20% des candidats répondent correctement à cette question. Les autres ne se rendent pas compte qu'il y a quelque chose à démontrer pour la réciproque ou « démontrent » des résultats du type $A\vec{x} \bmod \vec{a} = \vec{0}$ implique $A|\vec{x}| \bmod \vec{a} = \vec{0}$! Certains invoquent même des noyaux, croyant raisonner dans des espaces vectoriels ou des modules (hors programme). Mais $\mathcal{N}_{\vec{c}}$ n'a ici aucune structure algébrique particulière.

Question 1.7.

Puisque A est unimodulaire, A est inversible dans $\mathcal{M}_n(\mathbb{Z})$. De plus, $|\det(A^{-1}D)| = |\det(D)| = \prod_i a_i \neq 0$. D'après la question 1.5, il existe donc une unique décomposition

$A^{-1}D = HQ$ où H est la forme d'Hermite de $A^{-1}D$. On suppose ici que pour tout i, $H(i,i) = c_i > 0$.

On commence par vérifier l'injectivité. D'après le résultat de la question 1.6, il suffit de montrer que s'il existe $\vec{x} \in \mathbb{Z}^n$ tel que $A\vec{x} \bmod \vec{a} = \vec{0}$ avec $\forall i, -c_i < x_i < c_i$, alors $\vec{x} = \vec{0}$. Supposons qu'il existe un tel $\vec{x}$ avec $\vec{x} \neq \vec{0}$. Il existe alors $\vec{y} \in \mathbb{Z}^n$ tel que $A\vec{x} = D\vec{y}$, c'est-à-dire $\vec{x} = A^{-1}D\vec{y}$. On pose $\vec{z} = Q\vec{y}$ et on obtient $\vec{x} = H\vec{z}$ avec $\vec{z} \neq \vec{0}$. Soit alors i_0 le plus petit indice tel que $z_{i_0} \neq 0$. Puisque H est triangulaire inférieure, il vient :

$$x_{i_0} = \sum_{j=0}^{i_0} H(i_0, j) z_j = H(i_0, i_0) z_{i_0} = c_{i_0} z_{i_0} \, .$$

Donc x_{i_0} est un multiple non nul de c_{i_0} ce qui est impossible puisque $-c_{i_0} < x_{i_0} < c_{i_0}$. Donc $\vec{x} = \vec{0}$ et la restriction de $A_{\vec{a}}$ à $\mathcal{N}_{\vec{c}}$ est injective.

Pour la bijectivité, sachant que l'injectivité est vérifiée, il suffit de montrer que les deux ensembles $\mathcal{N}_{\vec{c}}$ et $\mathcal{N}_{\vec{a}}$ ont même cardinal. Comme A et Q sont unimodulaires, l'égalité $\det(A^{-1}D) = \det(HQ)$ entraîne l'égalité $|\det(D)| = |\det(H)|$. Comme D est diagonale et H triangulaire, on en déduit :

$$|\prod_i D(i,i)| = |\prod_i H(i,i)| \quad \text{c'est-à-dire} \quad \prod_i a_i = \prod_i c_i \, .$$

Remarque On peut également démontrer la surjectivité directement, mais les calculs sont légèrement plus lourds.

Question 1.8.

On suppose que $\det(A) \wedge a = 1$. Si $\det(A) = 0$ alors $a = 1$ et $\mathcal{N}_{\vec{a}} = \{\vec{0}\}$. Il est alors immédiat que la restriction de $A_{\vec{a}}$ à $\{\vec{0}\}$ est injective.

Supposons donc $\det(A) \neq 0$ et écrivons $A = HQ$ où H est la forme d'Hermite de A et Q est unimodulaire (d'inverse Q^{-1} entier donc). Puisque $|\det(A)| = |\det(H)| = \prod_i H(i,i)$ et $\det(A) \wedge a = 1$, on a $H(i,i) \wedge a = 1$ pour tout i. Soit à présent $\vec{x} \in \mathbb{Z}^n$ tel que $\forall i, -c_i < x_i < c_i$ et $A\vec{x} \bmod \vec{a} = \vec{0}$, c'est-à-dire $A\vec{x} = a\vec{y}$ avec $\vec{y} \in \mathbb{Z}^n$ puisque $\vec{a} = (a, \ldots, a)$. En posant $\vec{z} = Q\vec{x}$, on a $H\vec{z} = a\vec{y}$. Comme H est triangulaire inférieure, on obtient $H(0,0)z_0 = ay_0$: $H(0,0)$ divise ay_0 et donc y_0 puisque $H(0,0)$ est premier avec a (propriété de Gauss). On en déduit que $z_0 = aw_0$ pour un certain $w_0 \in \mathbb{Z}$. En procédant par récurrence, on montre de même que $z_i = aw_i$ avec $w_i \in \mathbb{Z}$, c'est-à-dire finalement $\vec{z} = a\vec{w}$ avec $\vec{w} \in \mathbb{Z}^n$. Comme $\vec{x} = Q^{-1}\vec{z}$, on en déduit que $\vec{x} = aQ^{-1}\vec{w} = a\vec{v}$ avec $\vec{v} \in \mathbb{Z}^n$. Enfin, puisque $\vec{c} = \vec{a}$, on a $\forall i, -a_i < x_i < a_i$ donc $\vec{v} = \vec{0}$ et $\vec{x} = \vec{0}$. On a ainsi montré que la restriction de $A_{\vec{a}}$ à $\mathcal{N}_{\vec{a}}$ est injective.

Supposons à présent que $A_{\vec{a}}$ soit surjective. Considérons $\vec{e}^{\,i} \in \mathcal{N}_{\vec{a}}$ tel que $e_i^i = 1$ et $e_j^i = 0$ si $i \neq j$. Il existe donc $\vec{f}^{\,i} \in \mathbb{Z}^n$ tel que $A\vec{f}^{\,i} \bmod \vec{a} = \vec{e}^{\,i}$, c'est-à-dire qu'il existe $\vec{g}^{\,i} \in \mathbb{Z}^n$ tel que $A\vec{f}^{\,i} = \vec{e}^{\,i} + a\vec{g}^{\,i}$. En regroupant ces égalités de façon matricielle, on obtient $AB = I + aC$ où B est la matrice dont les colonnes sont les $\vec{f}^{\,i}$ et C est la matrice dont les colonnes sont les $\vec{g}^{\,i}$. On a alors $\det(A)\det(B) = \det(I + aC)$. Ce dernier déterminant est un polynôme en a (voir l'équation (1)) dont le terme constant est la valeur du polynôme pour $a = 0$, c'est-à-dire $\det(I) = 1$. Par conséquent, $\det(I + aC) = 1 + ap$ où p est un entier. Finalement, $\det(A)\det(B) = 1 + ap$ ce qui prouve $\det(A) \wedge a = 1$ (propriété de Bezout).

En conclusion, dans le cas où $\vec{a} = (a, \dots, a)$, la restriction de $A_{\vec{a}}$ à $\mathcal{N}_{\vec{a}}$ est bijective si et seulement si $\det(A) \wedge a = 1$.

Remarques Pour la première partie de la question, on peut également utiliser la transposée de la matrice des cofacteurs, comme à la question 1.4. On a $\tilde{A}^T A\vec{x} = a\tilde{A}^T\vec{y}$, c'est-à-dire $\det(A)\vec{x} = a\vec{w}$ avec $\vec{w} = \tilde{A}^T\vec{y}$. Puisque $\det(A)$ est premier avec a, on obtient qu'il existe $\vec{v} \in \mathbb{Z}^n$ tel que $\vec{x} = a\vec{v}$, en raisonnant composante par composante. On conclut comme précédemment.

En fait, on obtient une solution plus courte et élégante à cette question en utilisant la notion (hors-programme) de module sur un anneau commutatif. En effet, $B = A_{\vec{a}}$ est une application linéaire sur le $\mathbb{Z}/a\mathbb{Z}$-module $(\mathbb{Z}/a\mathbb{Z})^n$. On a donc $B\tilde{B}^T = \det(B)I$, où $\tilde{B}$ est la matrice des co-facteurs de B. On en déduit que B est bijective si et seulement si $\det(B) = \det(A) \bmod a$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$.

Enfin, pour être vraiment complet sur la bijectivité de la restriction de $A_{\vec{a}}$ dans $\mathcal{N}_{\vec{a}}$, il faudrait considérer le cas où $\vec{a}$ et $\vec{c}$ sont quelconques (mais avec $\prod_i a_i = \prod_i c_i$), et la matrice A quelconque, et donner une condition nécessaire et suffisante. Une telle étude est possible mais non demandée ici.

Partie 2. Quelques propriétés des carrés latins

Question 2.1.

Considérons le carré latin de taille 3 suivant :

$$\begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}.$$

Dans le magma associé, $1 \star 0 = 2$ donc ni 0 ni 1 ne sont élément neutre et $2 \star 2 = 1$ donc 2 n'est pas élément neutre.

Soit A un carré latin de taille n. Pour trouver un carré latin B équivalent à A et tel que le magma associé à B ait 0 comme élément neutre, il suffit de réordonner les lignes de A pour que la colonne d'indice 0 soit $(0, 1, \dots, n-1)$, puis de réordonner les colonnes (sans toucher à celle d'indice 0) pour que la ligne d'indice 0 soit $(0, 1, \dots, n-1)$. Formellement, on définit la permutation g de $\mathcal{N}_n$ par $A(g(i), 0) = i$ ce qui est possible car tous les éléments de $\mathcal{N}_n$ apparaissent une et une seule fois dans la colonne d'indice 0. Puis, on définit la permutation h de $\mathcal{N}_n$ par $A(g(0), h(i)) = i$. Puisque $A(g(0), 0) = 0$, on a $h(0) = 0$. On définit alors le carré latin B équivalent à A par $B(i,j) = A(g(i), h(j))$. Par construction, $B(0,j) = A(g(0), h(j)) = j$ et $B(i,0) = A(g(i), h(0)) = A(g(i), 0) = i$, ce qui entraîne que le magma associé à B admet 0 pour élément neutre.

Dans la suite du corrigé, on appelle *carré latin normalisé*, un carré latin dont le magma associé admet 0 comme élément neutre.

Remarque Il n'est pas vrai qu'une classe d'équivalence ne contient qu'un seul carré latin normalisé, voir par exemple l'étude des carrés latins de taille 4 à la question 2.4.

Pour $n = 1$ et $n = 2$, il est évident qu'il n'y a qu'une classe d'équivalence. Considérons le cas $n = 3$. Un carré latin normalisé C de taille 3 a pour forme :

$$C = \begin{pmatrix} 0 & 1 & 2 \\ 1 & * & * \\ 2 & * & * \end{pmatrix} \implies C = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} . \tag{2}$$

En effet, on constate qu'on a nécessairement $C(2, 1) = 0$ et $C(1, 2) = 0$, et on en déduit que $C(1, 1) = 2$ et $C(2, 2) = 1$. Il n'y a donc qu'un seul carré latin normalisé de taille 3. D'après la première partie de la question, on en déduit l'existence d'une unique classe d'équivalence pour $n = 3$.

Pour $n = 1$, il n'y a qu'un carré latin, et pour $n = 2$, on voit aisément qu'il y en a deux. Considérons le cas $n = 3$ et le carré latin C défini comme en (2). On peut par inspection générer les 12 carrés latins de taille 3. On peut également se dire que si on renomme bijectivement les éléments de la ligne d'indice 0, qu'on fait le choix de l'élément d'indice $(1, 0)$, on se trouve dans la même situation que pour le carré C : il y a une et une seule façon de compléter le carré en un carré latin. Il y a donc $3 \times 2 \times 2 = 12$ carrés latins de taille 3.

Remarque On peut généraliser l'argument précédent pour compter le nombre de carrés latins dans une classe d'équivalence et ce en toute dimension. Étant donné un carré latin A normalisé de taille n et deux permutations g et h de $\mathcal{N}_n$ avec $h(0) = 0$, définissons $A_{g,h}(i, j) = A(g^{-1}(i), h^{-1}(j))$ pour tout (i, j). D'après l'étude précédente, l'application qui à A, g et h associe $A_{g,h}$ est surjective dans l'ensemble des carrés latins de taille n. Soient g_a, g_b, h_a, h_b, avec $h_a(0) = h_b(0) = 0$, permutations de $\mathcal{N}_n$, et A et B deux carrés latins normalisés de taille n tels que $A_{g_a,h_a} = B_{g_b,h_b}$. Pour tout i, $A(i, 0) = B(i, 0) = i$, et pour tout j, $A(0, j) = B(0, j) = j$. On a alors :

$$g_a^{-1}(i) = A(g_a^{-1}(i), 0) = A_{g_a,h_a}(i, 0) = B_{g_b,h_b}(i, 0) = B(g_b^{-1}(i), 0) = g_b^{-1}(i) .$$

Donc $g_a = g_b$ (notons à présent cette permutation g). De même :

$$h_a^{-1}(j) = A(0, h_a^{-1}(j)) = A_{g,h_a}(g(0), j) = B_{g,h_b}(g(0), j) = B(0, h_b^{-1}(j)) = h_b^{-1}(j) .$$

Ainsi $h_a = h_b$ (notons cette permutation h). Finalement, on a :

$$A(i, j) = A_{g,h}(g(i), h(j)) = B_{g,h}(g(i), h(j)) = B(i, j) .$$

Les deux carrés latins A et B sont égaux. L'application qui à A, g et h associe $A_{g,h}$ est donc injective. On déduit de ce raisonnement que le nombre de carrés latins de taille n est égal au nombre de carrés latins normalisés de taille n multiplié par $\mathrm{Card}(\mathfrak{S}_n) \times \mathrm{Card}(\mathfrak{S}_{n-1}) = n!(n-1)!$. Pour $n = 3$, on a donc $3!2! = 12$ carrés latins et pour $n = 4$, on en a $4!3!4 = 576$ (car on verra à la question 2.4 qu'il y a 4 carrés latins normalisés différents).

Question 2.2.

Soit n un entier strictement positif et soit la matrice carrée A de taille n définie par $A(i, j) = i + j \bmod n$. Le magma associé est le groupe cyclique $G = \mathbb{Z}/n\mathbb{Z} = (\mathcal{N}_n, +)$ où +

est l'addition modulo n. Quel que soit $g \in G$, l'application de G dans G qui à g' associe $g+g'$ (respectivement $g'+g$) est une bijection : dans chaque ligne et chaque colonne de A, chaque élément de G apparaît donc une et une seule fois, et A est un carré latin. Il existe donc des carrés latins de n'importe quelle taille.

Remarque Plus généralement, soit $(G, \star)$ un groupe fini d'ordre n avec $G = \{g_0, \cdots, g_{n-1}\}$. La matrice carrée A de taille n définie par $A(i,j) = k$ si $g_i \star g_j = g_k$ est alors un carré latin. Son magma associé est isomorphe à $(G, \star)$. Les questions suivantes donnent quelques indications sur les cas où les magmas associés aux carrés latins sont ou ne sont pas des groupes. Peu de candidats ont été à l'aise avec ces concepts.

Question 2.3.

On a $x \star y = f(g(x) \bullet h(y))$. On en déduit :

$$\begin{aligned}
(x \star y) \star z &= f(g(x \star y) \bullet h(z)) = f\left[gf[g(x) \bullet h(y)] \bullet h(z)\right] \\
x \star (y \star z) &= f(g(x) \bullet h(y \star z)) = f\left[g(x) \bullet hf[g(y) \bullet h(z)]\right] .
\end{aligned}$$

De par l'associativité de $(H, \star)$, on a $f^{-1}((x \star y) \star z) = f^{-1}(x \star (y \star z))$. On obtient donc, quels que soient x, y et z dans H :

$$gf[g(x) \bullet h(y)] \bullet h(z) = g(x) \bullet hf[g(y) \bullet h(z)] . \tag{3}$$

Soit e l'élément neutre de $(G, \bullet)$. En posant $x = g^{-1}(e)$ et $z = h^{-1}(e)$ dans l'équation précédente, on obtient $gfh(y) = hfg(y)$ pour tout y. Exprimons à présent $hfg(x \star y)$:

$$\begin{aligned}
hfg(x \star y) &= hfg(f(g(x) \bullet h(y))) = hfgf(g(x) \bullet h(y)) \\
&= hf(g(x) \bullet hfg(y)) \\
&= gfh(x) \bullet hfg(y) \\
&= hfg(x) \bullet hfg(y) .
\end{aligned}$$

On passe de la première à la deuxième ligne en utilisant (3) pour z tel que $h(z) = e$. On passe de la deuxième à la troisième ligne en utilisant (3) avec $g(x) = e$, $y = x$ et $z = fg(y)$.

Question 2.4.

On peut par inspection directe construire tous les carrés latins normalisés de taille 4, c'est-à-dire ceux dont le magma associé admet 0 pour élément neutre. On obtient les quatre carrés latins suivants :

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}, \; B = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 1 & 0 \\ 3 & 2 & 0 & 1 \end{pmatrix}, \; C = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}, \; D = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 0 & 2 \\ 2 & 0 & 3 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}.$$

Il s'agit maintenant de déterminer si certains de ces carrés latins sont équivalents. Il est évidemment hors de question de tester toutes les permutations et tous les renommages possibles, il faut donc avoir le bon réflexe d'utiliser certains des résultats précédents. La fin de la question (trouver un carré latin qui ne soit pas équivalent à un carré latin associé à un groupe) met la puce à l'oreille et dirige la recherche vers l'étude des groupes.

Certains de ces carrés latins sont nécessairement associés à des groupes. En effet, on doit retrouver les tables des deux groupes finis d'ordre 4, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. De plus, si d'autres carrés latins normalisés leur sont équivalents, il suffit de vérifier qu'ils leur sont isomorphes ou même de les identifier directement comme groupes. En effet, d'après la question 2.3, deux magmas, associés à des carrés latins équivalents (c'est ce qu'exprime la relation $x \star y = f(g(x) \bullet h(y)))$, sont isomorphes (c'est ce qu'exprime la relation $F(x \star y) = F(x) \bullet F(y)$ avec $F = hfg$), dès lors que l'un possède un élément neutre (par exemple si le carré latin associé est normalisé) et l'autre une loi associative (par exemple si c'est un groupe). En particulier, tout magma associé à un carré latin normalisé équivalent à un carré latin associé à un groupe est également un groupe.

Revenons à l'analyse des matrices A, B, C et D. On commence par remarquer que C est associé au groupe $\mathbb{Z}/4\mathbb{Z} = (\mathcal{N}_4, +)$ où $+$ est l'addition modulo 4. Considérons maintenant le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = (\mathcal{N}_2 \times \mathcal{N}_2, \star)$ avec $(a,b) \star (c,d) = (a+c, b+d)$ où $+$ est l'addition modulo 2. Sa table est donnée par :

$$\begin{array}{c|cccc}
\star & (0,0) & (0,1) & (1,0) & (1,1) \\
\hline
(0,0) & (0,0) & (0,1) & (1,0) & (1,1) \\
(0,1) & (0,1) & (0,0) & (1,1) & (1,0) \\
(1,0) & (1,0) & (1,1) & (0,0) & (0,1) \\
(1,1) & (1,1) & (1,0) & (0,1) & (0,0)
\end{array}.$$

On constate que c'est exactement le carré latin A en renommant les éléments dans $\mathcal{N}_4$ de manière adéquate, $(0,0)$ en 0, $(0,1)$ en 1, $(1,0)$ en 2 et $(1,1)$ en 3. Le groupe $\mathbb{Z}/4\mathbb{Z}$ n'étant pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, le carré latin A n'est pas équivalent au carré latin C.

Il reste à identifier les carrés latins B et D. S'ils sont équivalents à A ou C, puisque leur magma associé possède 0 comme élément neutre et que A et C sont associés à des groupes, ils sont eux mêmes associés à des groupes. On peut par exemple considérer les sous-ensembles engendrés par un élément comme première indication de leur structure.

Dans B, on voit que $1 \star 1 = 0$, donc 1 est d'ordre 2 si B est un groupe. On a $2 \star 2 = 1$, $1 \star 2 = 3$ et $3 \star 2 = 0$. Donc si B est un groupe, 2 est d'ordre 4, et B est isomorphe à $\mathbb{Z}/4\mathbb{Z}$. On essaie l'isomorphisme qui renomme 1 en 2 (éléments d'ordre 2), 2 en 1 (éléments d'ordre 4) et on laisse 3 en 3, puis on permute les lignes 1 et 2, ainsi que les colonnes 1 et 2. On obtient successivement les carrés :

$$\begin{pmatrix} 0 & 2 & 1 & 3 \\ 2 & 0 & 3 & 1 \\ 1 & 3 & 2 & 0 \\ 3 & 1 & 0 & 2 \end{pmatrix} \text{ puis } \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}.$$

On reconnaît le carré C, associé à $\mathbb{Z}/4\mathbb{Z}$.

Dans D, on calcule $1 \star 1 = 3$, $3 \star 1 = 2$, $2 \star 1 = 0$, donc à nouveau un élément potentiellement d'ordre 4. Si D est associé à un groupe, il serait donc isomorphe à $\mathbb{Z}/4\mathbb{Z}$. Il reste à identifier l'élément qui serait d'ordre 2, on voit que c'est 3. On renomme 3 en 2, puis on permute les lignes 2 et 3, et les colonnes 2 et 3 et on obtient :

$$\begin{pmatrix} 0 & 1 & 3 & 2 \\ 1 & 2 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 3 & 1 & 0 \end{pmatrix} \text{ puis } \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix}.$$

On reconnaît à nouveau C, associé à $\mathbb{Z}/4\mathbb{Z}$.

Il y a donc uniquement deux classes d'équivalence pour $n = 4$, un carré latin normalisé associé à un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et trois carrés latins normalisés associés à des groupes isomorphes à $\mathbb{Z}/4\mathbb{Z}$.

Pour trouver un carré latin qui ne soit pas équivalent à un carré latin associé à un groupe, il faut donc chercher avec $n \geq 5$. Encore une fois, il est exclu de chercher ce carré latin par énumération, à l'aveugle, à moins de disposer d'un ordinateur. Mais on peut, par quelques raisonnements simples diriger la recherche vers une solution.

Tout d'abord, on peut évidemment limiter la recherche aux carrés latins normalisés. Si un carré latin normalisé est associé à un groupe, il possède déjà quelques propriétés liées à sa structure : sa loi est associative (ce qui est un peu lourd à vérifier) et les inverses à droite sont les inverses à gauche (donc les 0 sont placés symétriquement par rapport à la diagonale dans la table du groupe). Il suffit donc de construire un carré latin normalisé tel que les 0 ne sont pas placés symétriquement par rapport à la diagonale. En voici un de taille 5 :

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 & 0 \\ 2 & 0 & 1 & 4 & 3 \\ 3 & 2 & 4 & 0 & 1 \\ 4 & 3 & 0 & 1 & 2 \end{pmatrix}.$$

On peut aussi raisonner directement avec la valeur $n = 5$. En effet, tout groupe d'ordre 5 est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Ce groupe a de multiples propriétés : il est commutatif (sa table est donc symétrique par rapport à la diagonale) et tout élément, sauf le neutre, est d'ordre 5. Pour construire un carré latin de taille 5 qui ne soit pas associé à $\mathbb{Z}/5\mathbb{Z}$, il suffit donc par exemple de construire un carré latin normalisé ayant un 0 sur la diagonale en position autre que $(0, 0)$ (élément d'ordre 2 si le carré est associé à un groupe). En voici un :

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 4 & 2 & 3 \\ 2 & . & 0 & . & . \\ 3 & . & . & 0 & . \\ 4 & . & . & . & 0 \end{pmatrix} \text{ complété (de façon unique) en } \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 4 & 2 & 3 \\ 2 & 3 & 0 & 4 & 1 \\ 3 & 4 & 1 & 0 & 2 \\ 4 & 2 & 3 & 1 & 0 \end{pmatrix}.$$

Remarque Dans leur immense majorité, les candidats n'ont pas compris comment aborder cette question. Ils ne pensent pas à utiliser la question 2.3 ou leurs connaissances sur les groupes d'ordre 4.

Question 2.5.

Remarquons pour commencer que les permutations σ_j sont bien définies. Comme dans chaque ligne i, tous les éléments apparaissent une et une seule fois, il existe bien un unique indice (qu'on note $\sigma_j(i)$) tel que $B(i, \sigma_j(i)) = j$. De plus, si $i \neq i'$, $\sigma_j(i) \neq \sigma_j(i')$ car sinon l'élément j apparaîtrait deux fois dans la colonne $\sigma_j(i)$.

Pour montrer l'équivalence demandée, il est plus simple de raisonner deux fois par la contraposée. Supposons qu'il existe j tel que les $A(i, \sigma_j(i))$ ne soient pas tous distincts. Il existe donc $i \neq i'$, tels que $A(i, \sigma_j(i)) = A(i', \sigma_j(i'))$. Puisque $B(i, \sigma_j(i)) = j = B(i', \sigma_j(i'))$, on a $C(i, \sigma_j(i)) = C(i', \sigma_j(i'))$, donc A et B ne sont pas orthogonaux. Réciproquement, supposons que A et B ne soient pas orthogonaux. Il existe donc $(i, j) \neq (k, l)$ tels que $A(i, j) = A(k, l)$ et $B(i, j) = B(k, l) = p$. On a donc $j = \sigma_p(i)$ et $l = \sigma_p(k)$. Ainsi $A(i, \sigma_p(i)) = A(k, \sigma_p(k))$. On ne peut avoir $i = k$, sinon on aurait $j = l$ et $(i, j) = (k, l)$. Donc, $i \neq k$ et les $A(., \sigma_p(.))$ ne sont pas tous distincts.

Soit A le carré latin associé au groupe $\mathbb{Z}/2p\mathbb{Z}$. Supposons que A admette un orthogonal B. Soit σ la permutation telle que $B(i, \sigma(i)) = 0$ pour tout i : les éléments $A(i, \sigma(i))$ sont tous distincts, leur somme est donc égale à la somme de tous les éléments du groupe. On a donc :

$$\sum_{i \in \mathcal{N}_{2p}} A(i, \sigma(i)) \bmod 2p = \sum_{i=0}^{2p-1} i \bmod 2p = p(2p-1) \bmod 2p = p \bmod 2p\,.$$

Par ailleurs, on a $A(i, \sigma(i)) = i + \sigma(i) \bmod 2p$ par définition du carré associé et, puisque σ est une permutation, on a :

$$\sum_{i \in \mathcal{N}_{2p}} A(i, \sigma(i)) \bmod 2p = 2 \sum_{i \in \mathcal{N}_{2p}} i \bmod 2p = 0 \bmod 2p\,.$$

On déduit de cette contradiction que A ne peut avoir d'orthogonal. Cette propriété s'étend à tout carré latin équivalent à un carré latin associé à un groupe isomorphe à $\mathbb{Z}/2p\mathbb{Z}$ car il est immédiat de voir qu'un carré latin équivalent à un carré latin possédant un orthogonal possède également un orthogonal (il suffit d'appliquer à l'orthogonal les mêmes permutations de lignes, colonnes et éléments).

Question 2.6.

Soit $C = (A, B)$ un carré eulérien diagonal de taille n. Il suffit d'interpréter la paire $(A(i, j), B(i, j))$ comme la représentation en base n (ou modulo n) de l'élément $C(i, j)$. Soit donc D la matrice définie par $D(i, j) = A(i, j) + nB(i, j)$. Comme les couples $(A(i, j), B(i, j))$ sont tous distincts et que tous les $A(i, j)$ et $B(i, j)$ sont entre 0 et $n - 1$, on a $\{D(i, j) \mid i, j \in \mathcal{N}_n\} = \mathcal{N}_{n^2}$. D'autre part, A et B étant des carré latins diagonaux, les sommes des coefficients des lignes, des colonnes, de la diagonale et de l'anti-diagonale de D sont toutes égales à :

$$\sum_{i=0}^{n-1} i + n \sum_{i=0}^{n-1} i = (n+1) \sum_{i=0}^{n-1} i = \frac{(n+1)(n-1)n}{2}\,.$$

La matrice D est bien un carré magique.

Question 2.7.

Pour $n = 1$, $((0),(0))$ est un carré eulérien diagonal et (0) est un carré magique. Pour $n = 2$, les deux carrés latins sont :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Ils ne forment pas un carré eulérien. De plus, il ne saurait exister de carré magique de taille 2. En effet, dans une matrice de taille 2, la somme sur la ligne 0 et la somme sur la colonne 0 ne peuvent être égales puisque contenant un nombre commun et un nombre différent.

Pour $n = 3$, on construit facilement un carré latin orthogonal à l'unique carré latin normalisé (en plaçant des éléments différents dans les 3 cases correspondant à un même élément du carré normalisé, tout en garantissant la propriété de carré latin). On obtient les deux carrés latins orthogonaux suivants :

$$\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \text{ et } \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{pmatrix}.$$

Il n'existe pas de carré latin diagonal de taille 3, comme illustré ci-dessous :

$$\begin{pmatrix} \square & & ? \\ & \Diamond & \\ & & \triangle \end{pmatrix}.$$

Une fois une diagonale déterminée, on ne peut définir l'élément à l'intersection des trois ensembles constitués d'une ligne, d'une colonne et de l'autre diagonale. En revanche, ceci ne prouve pas qu'il n'existe pas de carré magique de taille 3. Essayons d'en construire un. Si un tel carré existe, calculons la somme S des éléments de chacune des lignes, colonnes et diagonales. En effectuant la somme des lignes et colonnes, on compte deux fois chaque élément et six fois la somme S. On a donc $6S = 2\sum_{i=0}^{8} i = 72$, soit $S = 12$. Voici tous les ensembles constitués de trois éléments différents dans $\mathcal{N}_9$ dont la somme vaut 12 :

$$(0,4,8),\ (0,5,7),\ (1,3,8),\ (1,4,7),\ (1,5,6),\ (2,3,7),\ (2,4,6) \text{ et } (3,4,5)\,.$$

On doit donc retrouver ces 8 sous-ensembles sur les 3 lignes, les 3 colonnes et les 2 diagonales du carré magique. Un seul élément (l'élément diagonal) doit appartenir à 4 de ces ensembles : c'est donc 4 qui doit être placé au centre. Les éléments dans les angles doivent apparaître dans 3 ensembles, ce sont donc 1, 3, 5 et 7. Puisque 1 et 7 sont dans le même ensemble comprenant 4 (l'élément central), on en déduit qu'ils sont sur la même diagonale. Le placement des autres éléments en découle et on obtient (par exemple) le carré magique suivant :

$$\begin{pmatrix} 1 & 8 & 3 \\ 6 & 4 & 2 \\ 5 & 0 & 7 \end{pmatrix}.$$

Considérons maintenant le cas $n = 4$. Comme on l'a vu à la question 2.4, tous les carrés latins normalisés de taille 4 sont associés à un groupe, soit $\mathbb{Z}/4\mathbb{Z}$, soit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Par ailleurs, d'après l'analyse faite à la question 2.5, tout carré latin équivalent à un carré latin possédant un orthogonal en possède un, et un carré latin équivalent à un carré latin associé à un groupe cyclique d'ordre pair ne peut avoir d'orthogonal. Pour chercher un carré latin eulérien, il faut donc essayer de le construire à partir du carré associé à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, soit le A de la question 2.4. Comme A n'est pas diagonal, pour faire d'une pierre deux coups (la construction d'un carré eulérien et la construction d'un carré eulérien diagonal), on peut raisonner sur A' obtenu en insérant la colonne d'indice 0 entre les colonnes d'indice 2 et 3 :

$$A' = \begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{pmatrix} .$$

On veut construire A'' orthogonal à A'. D'après la propriété de la question 2.5, on doit placer quatre éléments distincts dans A'' aux places occupées par 0 dans A' (et la position de ces éléments dans ces 4 places n'importe pas, à un renommage près). On n'a alors plus le choix pour les éléments diagonaux. Et finalement, les autres éléments sont également imposés. On obtient donc successivement :

$$A'' = \begin{pmatrix} . & . & 0 & . \\ 1 & . & . & . \\ . & 2 & . & . \\ . & . & . & 3 \end{pmatrix} = \begin{pmatrix} 2 & . & 0 & 1 \\ 1 & 0 & 3 & . \\ . & 2 & 1 & . \\ 0 & . & . & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 0 & 1 \\ 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix}$$

qui est bien orthogonal à A' et diagonal. En utilisant le procédé de la question 2.6, on obtient le carré magique suivant :

$$\begin{pmatrix} 1 & 2 & 0 & 3 \\ 0 & 3 & 1 & 2 \\ 3 & 0 & 2 & 1 \\ 2 & 1 & 3 & 0 \end{pmatrix} + 4 \begin{pmatrix} 2 & 3 & 0 & 1 \\ 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 9 & 14 & 0 & 7 \\ 4 & 3 & 13 & 10 \\ 15 & 8 & 6 & 1 \\ 2 & 5 & 11 & 12 \end{pmatrix} .$$

Question 2.8.

On a :

$$\begin{aligned} (\forall i, \forall j \neq k,\ ai + bj \bmod n \neq ai + bk \bmod n) &\iff (\forall j \neq k,\ bj \bmod n \neq bk \bmod n) \\ &\iff b \text{ est un générateur de } \mathbb{Z}/n\mathbb{Z} \\ &\iff b \wedge n = 1 . \end{aligned}$$

On obtient de façon similaire :

$$\begin{aligned} (\forall i \neq l, \forall j,\ ai + bj \bmod n \neq al + bj \bmod n) &\iff a \wedge n = 1 \\ (\forall i \neq j,\ ai + bi \bmod n \neq aj + bj \bmod n) &\iff (a+b) \wedge n = 1 \\ (\forall i \neq j,\ ai + b(n-1-i) \bmod n \neq aj + b(n-1-j) \bmod n) &\iff (a-b) \wedge n = 1 . \end{aligned}$$

On en déduit que A est un carré latin si et seulement si $x \wedge n = 1$ pour $x \in \{a, b\}$, et que A est un carré latin diagonal si et seulement si $x \wedge n = 1$ pour $x \in \{a, b, a+b, a-b\}$.

Soient les deux carrés latins de taille n définis par $A(i,j) = (ai + bj) \bmod n$ et $B(i,j) = (ci+dj) \bmod n$. Puisque d est premier avec n, il existe un entier u tel que $(c+du) \bmod n = 0$. Les couples $(i, iu \bmod n), i \in \mathcal{N}_n$ sont les couples tels que $B(i, iu \bmod n) = 0$ (en d'autres termes, $\sigma_0(i) = iu \bmod n$ avec les notations de la question 2.5). Si (A,B) est un carré eulérien, alors les coefficients $A(i, iu \bmod n)$ sont tous distincts. On a alors :

$$(\forall i \neq j,\ ai + biu \bmod n \neq aj + bju \bmod n) \quad \Longleftrightarrow \quad (a+bu) \wedge n = 1\ .$$

Réciproquement, on vérifie que si $(a+bu) \wedge n = 1$, alors (A,B) est un carré eulérien. Cette condition est équivalente à celle demandée. En effet, si $(a+bu) \wedge n = 1$, on obtient que $(ad+bdu) \wedge n = 1$ puisque $d \wedge n = 1$. Par définition, on a $du = kn - c$ pour $k \in \mathbb{Z}$. On en déduit que $(ad - bc + bkn) \wedge n = 1$ ce qui entraîne $(ad-bc) \wedge n = 1$. Réciproquement, $(ad-bc) \wedge n = 1$ entraîne $(a+bu) \wedge n = 1$.

Comme indiqué dans l'énoncé, on peut obtenir le même résultat directement en utilisant la question 1.8. Soient deux carrés latins de taille n définis par $A(i,j) = (ai+bj) \bmod n$ et $B(i,j) = (ci+dj) \bmod n$. Le couple (A,B) est un carré eulérien si et seulement si l'application

$$\begin{array}{ccc} \mathcal{N}_n \times \mathcal{N}_n & \longrightarrow & \mathcal{N}_n \times \mathcal{N}_n \\ \begin{pmatrix} i \\ j \end{pmatrix} & \longmapsto & \begin{pmatrix} ai + bj \bmod n \\ ci + dj \bmod n \end{pmatrix} \end{array}$$

est une bijection, c'est-à-dire si et seulement si la restriction de $M_{\vec{a}}$ à $\mathcal{N}_{\vec{c}}$ est une bijection de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$ où :

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ et } \vec{c} = \vec{a} = \begin{pmatrix} n \\ n \end{pmatrix}\ .$$

D'après le résultat de la question 1.8, ceci est vérifié si et seulement si $\det(M) \wedge n = 1$, c'est-à-dire $(ad-bc) \wedge n = 1$ (en plus des conditions qui garantissent que A et B soient des carrés latins).

Question 2.9.

Définissons les matrices A et B de taille n par $A(i,j) = (2i+j) \bmod n$ et $B(i,j) = (i+2j) \bmod n$. En utilisant la question 2.8, on trouve que (A,B) est un carré eulérien diagonal dès que $2 \wedge n = 1$ et $3 \wedge n = 1$, c'est-à-dire si n n'est ni multiple de 2 ni de 3. En effet, il faut juste vérifier que $2 \wedge n = 1 \wedge n = (2+1) \wedge n = (2-1) \wedge n = (2*2 - 1*1) \wedge n = 1$. Dans le cas $n = 5$, on obtient :

$$A = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{pmatrix},\ B = \begin{pmatrix} 0 & 2 & 4 & 1 & 3 \\ 1 & 3 & 0 & 2 & 4 \\ 2 & 4 & 1 & 3 & 0 \\ 3 & 0 & 2 & 4 & 1 \\ 4 & 1 & 3 & 0 & 2 \end{pmatrix}.$$

Finalement, en appliquant le procédé de la question 2.6, on obtient le carré magique suivant :

$$\begin{pmatrix} 0 & 11 & 22 & 8 & 19 \\ 7 & 18 & 4 & 10 & 21 \\ 14 & 20 & 6 & 17 & 3 \\ 16 & 2 & 13 & 24 & 5 \\ 23 & 9 & 15 & 1 & 12 \end{pmatrix}.$$

Partie 3. Hyper-rectangles latins

Question 3.1.

On s'intéresse évidemment au cas $c \geq 0$ et $m \geq 0$. Si on veut placer n boules dans des boîtes de sorte que c d'entre elles en contiennent exactement m, alors il faut au moins cm boules, donc $cm \geq n$. Si chaque boîte ne peut contenir que m boules au plus, on ne pourra pas placer plus de dm boules dans d boîtes. On a donc $n \leq dm$. Réciproquement, si ces conditions sont vérifiées, il existe au moins une telle répartition : il suffit de placer m boules dans chacune des c premières boîtes, il en reste alors $(n - cm)$ à placer dans $(d - c)$ boîtes. On écrit $n - cm = qm + r$ (division euclidienne) avec $0 \leq r < m$. Si $r = 0$, on a $q \leq d - c$ et il suffit de placer m boules dans les q boîtes suivantes et 0 dans les $(d - c - q)$ autres. Si $r > 0$, on a $q \leq d - c - 1$ et on place m boules dans les q boîtes suivantes, r dans la suivante, et 0 dans les $(d - c - 1 - q)$ autres.

La procédure $\mathrm{P}(n, m, c, d)$ génère, une et une seule fois, **toutes** les répartitions possibles de n boules dans d boîtes distinctes de sorte que chaque boîte en contienne au plus m et qu'au moins c boîtes en contiennent exactement m. Pour que la procédure fonctionne correctement, il faut que les paramètres vérifient les conditions énoncées ci-avant. La démonstration se fait par récurrence sur d, le nombre de boîtes. On numérote les boîtes de 0 à $(d-1)$. On considère le remplissage de la boîte d'indice $(d - 1)$ de toutes les façons possibles et on remplit les premières récursivement.

Le cas $d = 1$ est élémentaire et l'algorithme a bien l'effet voulu. Plus précisément, comme $0 \leq c \leq 1$ et $cm \leq n \leq m$, deux cas sont possibles. Si $c = 0$, alors $n \leq m$ et on a bien une boîte remplie avec au plus m boules et si $c = 1$, on a $n = m$ et on a bien une boîte remplie avec exactement m boules.

Le cas général est plus compliqué. On choisit d'abord le nombre de boules $i \geq 0$ qu'on affecte à la dernière boîte d'indice $(d - 1)$. Deux cas sont possibles : $(i = m)$ ou $(i < m)$.

Si $i < m$, il faudra encore être capable de distribuer les boules restantes dans $(d - 1)$ boîtes en respectant les mêmes contraintes que précédemment. Par hypothèse de récurrence, la procédure qui permettra de remplir les autres boîtes est donc $\mathrm{P}(n - i, m, c, d - 1)$ et pour que cette procédure fasse son affectation correctement (tous les cas possibles une et une seule fois), il faut, toujours par hypothèse de récurrence, que $cm \leq n - i \leq m(d - 1)$, c'est-à-dire $n - (d - 1)m \leq i \leq n - cm$. Ceci explique les bornes de la boucle **Pour**. En fait, il faudrait rajouter l'inégalité $i \leq n$, mais puisque $c \geq 0$, la contrainte $i \leq n - cm$ l'assure.

Si $(i = m)$, il faut bien évidemment que m soit plus petit que n et il restera à placer $(n-m)$ boules dans $(d - 1)$ boîtes, chacune avec au plus m boules, et au moins $\max(0, c - 1)$ d'entre elles avec exactement m boules. C'est l'appel à $\mathrm{P}(n-m, m, \max(0, c-1), d-1)$ qui s'en charge. Les paramètres d'appel sont corrects car si $cm \leq n \leq dm$ alors $(c - 1)m \leq n - m \leq (d - 1)m$ et, de plus, $0 \leq n - m$.

Enfin, il faudrait stocker les solutions produites à un moment donné avant de remodifier le tableau « boîte ». Ceci peut se faire en fin de chaque séquence d'appels récursifs, c'est-à-dire lorsqu'on passe dans le test « **Si** $(d = 1)$ ».

Question 3.2.

Si $\vec{c}$ est une taille compatible avec p alors pour tout i, $\prod_{j\neq i} c_j$ est un multiple de p. Considérons i_0 tel que c_{i_0} soit divisible par α^m. Puisque $\prod_{j\neq i_0} c_j$ est un multiple de p, donc de α^r, $\prod_j c_j$ est un multiple de $\alpha^r \alpha^m = \alpha^{r+m}$. L'occurrence de α dans $\prod_j c_j$ est donc au moins $(r+m)$. On vérifie que la réciproque est vraie : si l'occurrence de α dans $\prod_j c_j$ est au moins $(r+m)$, alors l'occurrence de α dans $\prod_{j\neq i} c_j$ est au moins $r+m$ moins l'occurrence dans c_i, donc au moins r.

Si $r = 0$ alors α n'est facteur d'aucune composante de $\vec{c}$ sinon $\vec{c}$ ne serait pas élémentaire. La propriété à démontrer est donc bien vérifiée.

Si $r \neq 0$, l'occurrence de α dans $\prod_j c_j$ étant supérieure à r, l'occurrence maximale m de α dans une composante de $\vec{c}$ est strictement positive. Supposons que cette occurrence maximale ne soit atteinte que pour un seul indice i_0. Définissons alors $\vec{b}$ de la façon suivante :

$$b_i = \begin{cases} c_{i_0}/\alpha & \text{si } i = i_0 \\ c_i & \text{sinon.} \end{cases}$$

L'occurrence maximale m' de α dans une composante de $\vec{b}$ est $(m-1)$ et l'occurrence de α dans $\prod_j b_j$ est au moins $(r+m-1)$, donc plus grande que $(r+m')$. Donc pour tout i, l'occurrence de α dans $\prod_{j\neq i} b_j$ est au moins r. On en déduit que $\vec{b}$ est une taille compatible, ce qui contredit que $\vec{c}$ est élémentaire.

Enfin, supposons que l'occurrence de α dans $\prod_j c_j$ soit strictement plus grande que $(r+m)$. Considérons $\vec{b}$ obtenu en divisant par α une composante quelconque de $\vec{c}$ pour laquelle l'occurrence de α est strictement positive. D'après la seconde partie de la question, l'occurrence maximale m est atteinte pour au moins deux indices (on a supposé $\vec{c}$ élémentaire), donc l'occurrence maximale de α dans $\vec{b}$ est toujours égale à m. De plus, l'occurrence de α dans $\prod_j b_j$ est au moins $(r+m)$, donc l'occurrence de α dans $\prod_{j\neq i} b_j$ est au moins r. Donc $\vec{b}$ est toujours compatible avec p et $\vec{c}$ ne peut être élémentaire.

Question 3.3.

Soit $p = \alpha^r$ où α est un nombre premier. La question précédente indique que pour qu'une taille $\vec{c}$ soit compatible avec p, il faut que l'occurrence de α dans $\prod_j c_j$ soit exactement égale à $(r+m)$ où m, l'occurrence maximale de α dans une composante de $\vec{c}$, est atteinte au moins deux fois. Il reste à montrer la réciproque. Considérons une taille $\vec{c}$ vérifiant ces deux conditions (et sans autres facteurs dans les composantes de $\vec{c}$). L'occurrence de α dans $\prod_{j\neq i} c_j$, quel que soit i, est $(r+m-r_i)$ où r_i est l'occurrence de α dans c_i : l'inégalité $r_i \leq m$ garantit alors que α^r divise $\prod_{j\neq i} c_j$. Donc $\vec{c}$ est compatible avec p. Montrons à présent que $\vec{c}$ est élémentaire. Supposons qu'il existe $\vec{b} \neq \vec{c}$ compatible avec p tel que pour tout i, b_i divise c_i. Soit $t > 0$ défini par $\alpha^t = \prod_j c_j / \prod_j b_j$. L'occurrence de α dans $\prod_j b_j$ est donc $r+m-t$. Notons m' l'occurrence maximale de α dans une composante de $\vec{b}$. Puisque l'occurrence de α dans une composante de $\vec{c}$ est égale à m pour au moins deux composantes, on a $2m' \geq 2m - t$. On a alors :

$$r + m' \;\geq\; r + m - \frac{t}{2} \;>\; r + m - t\,.$$

Donc α n'apparaît pas assez souvent dans $\vec{b}$ et $\vec{b}$ n'est pas compatible avec p.

Pour générer toutes les tailles élémentaires pour $p = \alpha^r$, il suffit donc de considérer tous les cas possibles pour l'occurrence maximale m de α dans une composante de $\vec{c}$ et pour chacune de ces valeurs de m, d'utiliser $\mathrm{P}(r+m,\, m,\, 2,\, d)$, la répartition de $r+m$ boules (des copies de α) dans d boîtes (les composantes de $\vec{c}$) de sorte qu'au moins 2 boîtes (2 composantes) en contiennent exactement m, et que toute boîte en contienne au plus m.

Puisque l'occurrence de α dans $\prod_j c_j$ est exactement $r+m$, qu'elle est égale à m pour au moins deux composantes, et qu'elle est entre 0 et m pour toute composante, on a $2m \leq r+m \leq 2m+(d-2)m = dm$, c'est-à-dire $r/(d-1) \leq m \leq r$. Réciproquement, si ces inégalités sont vérifiées, les paramètres d'appel de $\mathrm{P}(r+m,\, m,\, 2,\, d)$ sont corrects car $0 \leq 2 \leq d$ et $2m \leq r+m \leq dm$. On en déduit le programme suivant :

> **Pour** m **de** $\lceil \frac{r}{d-1} \rceil$ **à** r
> $\mathrm{P}(r+m,\, m,\, 2,\, d)$;
> **FinPour**

Pour un entier p quelconque, on commence par remarquer que pour caractériser les tailles compatibles et les tailles élémentaires, il suffit de raisonner facteur premier par facteur premier. En effet, une taille $\vec{c}$ est compatible avec p si et seulement si pour tout i, p divise $\prod_{j\neq i} c_j$, c'est-à-dire si et seulement si pour tout facteur premier α d'occurrence r dans p, α^r divise $\prod_{j\neq i} c_j$, c'est-à-dire si et seulement si $\vec{c}$ est compatible avec α^r, pour tout facteur premier α d'occurrence r dans p. La même remarque est vraie également pour les tailles élémentaires. Une taille est élémentaire pour p si et seulement si elle est définie comme le produit (composante par composante) de tailles élémentaires, une pour chacun des α^r constituant p.

Il suffit donc de décomposer p en facteur premier, puis de générer toutes les tailles élémentaires pour chacun des facteurs premiers (comme précédemment) et de combiner toutes les solutions, c'est-à-dire de les multiplier entre elles (composante par composante) de toutes les façons possibles, en choisissant une solution par facteur premier. Pour ceci, il faudrait écrire un programme un peu plus complexe qui dans le test « **Si** $(d=1)$ » de la procédure P (donc à chaque fois qu'on a généré une taille élémentaire possible pour le facteur courant) passe à un facteur suivant et relance la procédure complète pour générer une taille élémentaire pour ce facteur, la multiplie à la précédente, ainsi jusqu'au dernier facteur. On ne demandait pas d'écrire ce programme.

Question 3.4.

Montrons que (i) est équivalent à (ii). Par définition, l'application $A_{\vec{a}}$ est un hyper-rectangle latin de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$ si et seulement si, pour tout i, $0 \leq i < d$, pour tout k, $0 \leq k < c_i$, la restriction de $A_{\vec{a}}$ à $\mathcal{N}_{\vec{c}}(i,k) = \{\vec{x} \in \mathcal{N}_{\vec{c}} \mid x_i = k\}$ est une multi-bijection dans $\mathcal{N}_{\vec{a}}$. La condition (ii) est alors évidemment vérifiée puisque restreinte aux cas où $k = 0$. Réciproquement, si (ii) est vérifiée, la condition (i) découle de la linéarité de l'application $A_{\vec{a}}$. En effet, notons $\vec{e}^{\,i}$ tel que $\vec{e}^{\,i}_i = 1$ et $\vec{e}^{\,i}_j = 0$ si $j \neq i$. L'ensemble $\mathcal{N}_{\vec{c}}(i,k)$ se déduit de l'ensemble $\mathcal{N}_{\vec{c}}(i,0)$ par une translation de $k\vec{e}^{\,i}$ et les images par $A_{\vec{a}}$ sont toutes décalées de $A\vec{e}^{\,i}$ (modulo $\vec{a}$). Deux éléments de $\mathcal{N}_{\vec{c}}(i,0)$ ont donc même image si et seulement si leurs translatés ont même image. La propriété de multi-bijection se transmet donc de $\mathcal{N}_{\vec{c}}(i,0)$ à $\mathcal{N}_{\vec{c}}(i,k)$.

L'application qui à $\vec{x} \in \mathcal{N}_{\vec{c}}(i,0)$ associe $\vec{y} \in \mathcal{N}_{\vec{b}}$ où $\vec{y}$ (resp. $\vec{b}$) est obtenu en supprimant la composante i de $\vec{x}$ (resp. $\vec{c}$) est une bijection. De plus, $A\vec{x} = B\vec{y}$. L'équivalence entre (ii) et (iii) en découle.

Question 3.5.

Un hyper-cube latin de taille $\vec{c}$ de dimension d est par définition un hyper-rectangle tel que toutes les multi-bijections (obtenues en considérant les restrictions à n'importe quelle « tranche ») sont des bijections. Par égalité des cardinaux des ensembles concernés, on a alors pour tout i, $\prod_{j \neq i} c_j = p$, donc $\prod_j c_j = pc_i$. On obtient donc que tous les c_i sont égaux et égaux à $\prod_j c_j / p = q$. Il s'ensuit que $p = q^{d-1}$.

Grâce au résultat de la question 3.4, on s'est ramené, par la condition (iii), à une condition portant sur des matrices carrées comme à la question 1.8. On va choisir par exemple $\vec{a} = \vec{c}$ pour se placer dans les mêmes conditions. Il suffit donc de construire une matrice entière de taille $(d-1) \times d$ telle que chacune de ses sous-matrices, obtenue en supprimant une colonne, a un déterminant premier avec p. On peut par exemple faire en sorte que ces déterminants soient tous égaux à 1 en considérant la matrice (rectangulaire) bi-diagonale suivante :

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 & 1 \end{pmatrix}.$$

Chacune des sous-matrices obtenues est une matrice constituée de deux blocs (l'un éventuellement vide), l'un triangulaire inférieur, l'autre triangulaire supérieur, avec des 1 sur la diagonale.

Remarque On peut retrouver ce résultat directement en l'interprétant dans $\mathbb{Z}/q\mathbb{Z}$, comme on l'a fait en dimension 2. L'application construite peut être vue comme l'application de $(\mathbb{Z}/q\mathbb{Z})^d$ dans $(\mathbb{Z}/q\mathbb{Z})^{d-1}$ qui à $\vec{x}$ associe $f(\vec{x}) = (x_0 + x_1 \bmod q, x_1 + x_2 \bmod q, \ldots, x_{d-2} + x_{d-1} \bmod q)$. Si on fixe une composante, par exemple x_i, il suffit de vérifier l'injectivité, c'est-à-dire de résoudre $f(\vec{x}) = \vec{0}$ en supposant $x_i = 0$ (pour la « tranche » $\mathcal{N}_{\vec{c}}(i,0)$). Les équations $x_{i-1} + x_i \bmod q = 0$ et $x_i + x_{i+1} \bmod q = 0$ impliquent $x_{i-1} = 0$ et $x_{i+1} = 0$, puis en résolvant le système de part en part à partir de x_{i-1} et de x_{i+1}, on obtient $\vec{x} = \vec{0}$.

Question 3.6.

D'après le résultat de la question 3.4, il suffit de vérifier que $A_{\vec{a}}$ est une multi-bijection de $\mathcal{N}_{\vec{c}}(i,0)$ dans $\mathcal{N}_{\vec{a}}$ pour tout i. Puisqu'on suppose que c'est vrai pour $i = d-1$, il suffit de le vérifier pour $0 \leq i < d-1$.

Considérons donc i, $0 \leq i < d-1$. Soit $\vec{y} \in \mathcal{N}_{\vec{a}}$. Comptons le nombre d'antécédents de $\vec{y}$ dans $\mathcal{N}_{\vec{c}}(i,0)$, c'est-à-dire le nombre de $\vec{x} \in \mathcal{N}_{\vec{c}}$ tels que $A\vec{x} \bmod \vec{a} = \vec{y}$ et $x_i = 0$. On a :

$$A\vec{x} \bmod \vec{a} = \vec{y} \Leftrightarrow \underline{A}\,\underline{\vec{x}} \bmod \underline{\vec{a}} = \underline{\vec{y}} \text{ et } (\underline{\vec{z}}.\underline{\vec{x}} + x_{d-1}) \bmod a_{d-1} = y_{d-1}$$

où $\underline{\vec{z}}$ est formé des $(d-1)$ premières composantes de la dernière ligne de A. Puisque $\underline{A}_{\underline{\vec{a}}}$ est un hyper-rectangle latin de dimension $(d-1)$ de $\mathcal{N}_{\underline{\vec{c}}}$ dans $\mathcal{N}_{\underline{\vec{a}}}$, le nombre d'éléments $\underline{\vec{x}} \in \mathcal{N}_{\underline{\vec{c}}}$ tels que $\underline{x}_i = 0$ et $\underline{A}\,\underline{\vec{x}} \bmod \underline{\vec{a}} = \underline{\vec{y}}$ ne dépend pas de $\underline{\vec{y}}$. Notons q_i ce nombre. Il reste à compter le nombre de valeurs x_{d-1}, entre 0 (inclus) et c_{d-1} (non inclus), telles que $x_{d-1} \bmod a_{d-1} = (y_{d-1} - \underline{\vec{z}}.\underline{\vec{x}}) \bmod a_{d-1}$. Puisque a_{d-1} divise c_{d-1}, il y a exactement c_{d-1}/a_{d-1} telles valeurs, quelle que soit la valeur de $x = (y_{d-1} - \underline{\vec{z}}.\underline{\vec{x}}) \bmod a_{d-1}$. Ce sont les valeurs $x + ka_{d-1}$, pour $0 \leq k < c_{d-1}/a_{d-1}$. Donc, $\vec{y}$ a $q_i c_{d-1}/a_{d-1}$ antécédents dans $\mathcal{N}_{\vec{c}}(i,0)$ et ce nombre ne dépend pas de $\vec{y}$. On a bien affaire à une multi-bijection.

Question 3.7.

Soient u, v et w trois entiers non nuls. Soit d le pgcd de u et v : on note $u = du'$ et $v = dv'$ où u' et v' sont premiers entre eux. On a alors :

$$u \wedge (vw) = (du') \wedge (dv'w) = d(u' \wedge (v'w))\,.$$

Mais u' est premier avec v' donc $u' \wedge (v'w) = u' \wedge w$. On en déduit l'égalité demandée :

$$u \wedge (vw) = (u \wedge v)(\frac{u}{u \wedge v} \wedge w)\,. \tag{4}$$

On va s'en servir de façon extensive pour les propriétés suivantes.

La première propriété est immédiate puisque le dénominateur de la fraction définissant $\vec{a}$ divise le numérateur. On a :

$$\prod_{i=0}^{d-2} a_i = \prod_{i=0}^{d-2} \frac{p \wedge \left(\prod_{j=i+1}^{d-1} c_j\right)}{p \wedge \left(\prod_{j=i+2}^{d-1} c_j\right)} = p \wedge \prod_{j=1}^{d-1} c_j = p\,,$$

où la dernière égalité provient de ce que $\vec{c}$ est compatible avec p. On a démontré la propriété (2).

Montrons la propriété (3). On a :

$$a_i(p \wedge \prod_{j=i+2}^{d-1} c_j) = p \wedge \prod_{j=i+1}^{d-1} c_j = (p \wedge c_{i+1}) \left(\frac{p}{p \wedge c_{i+1}} \wedge \prod_{j=i+2}^{d-1} c_j\right)$$

d'après l'identité (4) avec $u = p$ et $v = c_{i+1}$. Puisque $p \wedge \prod_{j=i+2}^{d-1} c_j$ est un multiple de $\left(\frac{p}{p\wedge c_{i+1}} \wedge \prod_{j=i+2}^{d-1} c_j\right)$, on en déduit que $p \wedge c_{i+1}$ est un multiple de a_i. Donc a_i divise à la fois p et c_{i+1}.

Montrons la propriété (4). On a :

$$a_i = \frac{p \wedge \prod_{j=i+1}^{d-1} c_j}{p \wedge \prod_{j=i+2}^{d-1} c_j} = \frac{(p \wedge c_{d-1})\left(\frac{p}{p\wedge c_{d-1}} \wedge \prod_{j=i+1}^{d-2} c_j\right)}{(p \wedge c_{d-1})\left(\frac{p}{p\wedge c_{d-1}} \wedge \prod_{j=i+2}^{d-2} c_j\right)} = \frac{\frac{p}{p\wedge c_{d-1}} \wedge \prod_{j=i+1}^{d-2} c_j}{\frac{p}{p\wedge c_{d-1}} \wedge \prod_{j=i+2}^{d-2} c_j}$$

qui est la formule pour $\underline{\vec{a}}$ avec $\underline{\vec{c}}$ et l'entier $p/(p \wedge c_{d-1})$.

Puisque $\vec{c}$ est une taille compatible, pour tout i, p divise $\prod_{j=0,j\neq i}^{d-1} c_j$, donc $p/(p \wedge c_{d-1})$ divise $\prod_{j=0,j\neq i}^{d-2} c_j$. Ainsi $\underline{\vec{c}}$ est une taille compatible avec $p/(p \wedge c_{d-1})$. Il reste à montrer la deuxième partie de la propriété (5). On a :

$$\prod_{j=0}^{i} a_j = \prod_{j=0}^{i} \left(\frac{p \wedge \prod_{k=j+1}^{d-1} c_k}{p \wedge \prod_{k=j+2}^{d-1} c_k} \right) = \frac{p \wedge \prod_{k=1}^{d-1} c_k}{p \wedge \prod_{k=i+2}^{d-1} c_k} = \frac{p}{p \wedge \prod_{k=i+2}^{d-1} c_k} .$$

Puisque $\vec{c}$ est une taille compatible avec p, p divise $\prod_{k\neq i+1} c_k$. Donc $p/(p \wedge \prod_{k=i+2}^{d-1} c_k)$ divise $\prod_{k=0}^{i} c_k$. On en déduit la propriété voulue.

Question 3.8.

Remarque Il y avait une petite imprécision ici dans le sujet, sans conséquence pour la suite. En effet, pour éviter des problèmes de signes et de division éventuelle par 0, il fallait supposer que $\mathrm{diag}(S)$ et $\vec{v} = (v_0, \ldots, v_{d-2})$ étaient à coefficients strictement positifs.

Supposons C de taille 2. D'après la question 1.3, on a :

$$C = \begin{pmatrix} v_0 & v_1 \\ s_0 & 0 \end{pmatrix} = HQ = \begin{pmatrix} h_0 & 0 \\ * & h_1 \end{pmatrix} Q$$

où $h_0 = v_0 \wedge v_1$. De plus, puisque Q est unimodulaire et que les coefficients diagonaux de H sont positifs, on a :

$$h_0 h_1 = \det(H) = |\det(C)| = s_0 v_1 .$$

Par conséquent, $h_1 = v_1 s_0 / h_0 = r_1 s_0 / r_0$. La propriété pour $d-1 = 2$ est donc démontrée.

Lorsque C est de taille $(d-1)$, on peut reproduire le schéma de calcul de la forme d'Hermite, en commençant par ne considérer que les deux dernières colonnes (celles d'indices $(d-2)$ et $(d-3)$) de sorte que la dernière composante de la ligne 0 soit 0. Puis on manipule les colonnes d'indices $(d-3)$ et $(d-4)$, puis $(d-4)$ et $(d-5)$, etc, de façon à rendre la ligne 0 nulle sauf le coefficient d'indice $(0,0)$. Par ce procédé, la matrice sera ramenée naturellement à une matrice triangulaire inférieure. Comme $\det(C)$ est non nul, la forme d'Hermite est unique (question 1.5) et la façon d'y parvenir est sans importance. Par rapport à l'algorithme de la question 1.3, ici on traite en fait le pgcd des coefficients de $\vec{v}$, non pas de façon globale, mais deux coefficients à la fois, en utilisant de façon cachée l'associativité du pgcd.

Détaillons ce procédé. Soit $r_{d-2} = v_{d-2}$ et r_i le coefficient apparaissant en position $(0,i)$, juste après que les manipulations de colonnes ont rendu nul le coefficient d'indice $(i+1)$ de la ligne 0. Juste avant ce changement, le coefficient d'indice $(i+1)$ valait r_{i+1} et celui d'indice i valait v_i. Par des manipulations adéquates des colonnes i et $(i+1)$, lorsque le coefficient d'indice $(i+1)$ devient 0, le pgcd de v_i et r_{i+1} apparaît en colonne i, on a donc $r_i = v_i \wedge r_{i+1}$.

Les matrices suivantes illustrent ce mécanisme :

$$\begin{pmatrix} v_0 & \dots & \boxed{v_i} & \boxed{r_{i+1}} & 0 & \dots & 0 \\ s_0 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & & & & & \vdots \\ \vdots & & \boxed{s_i} & \boxed{0} & \dots & \dots & 0 \\ 0 & \dots & 0 & * & h_{i+2} & \dots & 0 \\ \vdots & & \vdots & * & * & \ddots & \vdots \\ 0 & \dots & 0 & * & * & \dots & h_{d-2} \end{pmatrix} \Rightarrow \begin{pmatrix} v_0 & \dots & \boxed{r_i} & \boxed{0} & 0 & \dots & 0 \\ s_0 & 0 & \dots & \dots & \dots & \dots & 0 \\ 0 & \ddots & & & & & \vdots \\ \vdots & & \boxed{*} & \boxed{h_{i+1}} & \dots & \dots & 0 \\ 0 & \dots & 0 & * & h_{i+2} & \dots & 0 \\ \vdots & & \vdots & * & * & \ddots & \vdots \\ 0 & \dots & 0 & * & * & \dots & h_{d-2} \end{pmatrix}.$$

De plus, le déterminant de la matrice 2×2 définie par les colonnes i et $(i+1)$ et les lignes 0 et $(i+1)$ est laissé invariant (en valeur absolue) par ces opérations élémentaires. Il était égal (en valeur absolue) à $s_i r_{i+1}$, il vaut maintenant $r_i h_{i+1}$. Donc $h_{i+1} = (s_i r_{i+1})/r_i$. Après toutes ces manipulations successives, la matrice devient finalement triangulaire inférieure et h_0 est égal au dernier r_i restant, c'est-à-dire r_0.

Question 3.9.

Calculons r_i en fonction de r_{i+1}, en utilisant successivement l'identité (4) et le fait que a_i divise c_{i+1} (propriété (3) de la question 3.7). On a :

$$\begin{aligned} r_i &= r_{i+1} \wedge (a_i w_i) = r_{i+1} \wedge \left(a_i \frac{r_{i+1}}{r_{i+1} \wedge c_{i+1}} \right) \\ &= (r_{i+1} \wedge a_i) \left(\frac{r_{i+1}}{r_{i+1} \wedge a_i} \wedge \frac{r_{i+1}}{r_{i+1} \wedge c_{i+1}} \right) \\ &= (r_{i+1} \wedge a_i) \left(\frac{r_{i+1}}{r_{i+1} \wedge c_{i+1}} \right) = r_{i+1} \left(\frac{r_{i+1} \wedge a_i}{r_{i+1} \wedge c_{i+1}} \right) . \end{aligned} \tag{5}$$

En calculant h_{i+1}, on obtient alors :

$$h_{i+1} = \frac{r_{i+1} a_i}{r_i} = \frac{a_i (r_{i+1} \wedge c_{i+1})}{r_{i+1} \wedge a_i} .$$

On vérifie alors que h_{i+1} divise c_{i+1}. En effet :

$$\begin{aligned} h_{i+1} \text{ divise } c_{i+1} &\Leftrightarrow a_i (r_{i+1} \wedge c_{i+1}) \text{ divise } c_{i+1} (r_{i+1} \wedge a_i) \\ &\Leftrightarrow (a_i r_{i+1} \wedge a_i c_{i+1}) \text{ divise } (c_{i+1} r_{i+1} \wedge a_i c_{i+1}) . \end{aligned}$$

Mais a_i divise c_{i+1}, donc $a_i r_{i+1}$ divise $c_{i+1} r_{i+1}$ et $(a_i r_{i+1} \wedge a_i c_{i+1})$ divise $(c_{i+1} r_{i+1} \wedge a_i c_{i+1})$. Par conséquent, on a montré que pour tout $i > 0$, h_i divise c_i.

Montrons par récurrence descendante sur i, de $i = d-2$ à $i = 0$, que $r_i \prod_{j=0}^{i-1} a_j$ divise $\prod_{j=0}^{i} c_j$. Puisque $r_{d-2} = a_{d-2}$, le cas $i = d-2$ provient de la propriété (2) de la question 3.7 :

$$r_{d-2} \prod_{j=0}^{d-3} a_j = \prod_{j=0}^{d-2} a_j = p \text{ divise } \prod_{j=0}^{d-2} c_j ,$$

puisque $\vec{c}$ est une taille compatible avec p. Supposons que le résultat soit vrai pour $(i+1)$:

$$r_{i+1} \prod_{j=0}^{i} a_j \text{ divise } \prod_{j=0}^{i+1} c_j = c_{i+1} \prod_{j=0}^{i} c_j \,. \tag{6}$$

On sait que $\prod_{j=0}^{i} a_j$ divise $\prod_{j=0}^{i} c_j$ (propriété (5) de la question 3.7), donc il existe un entier λ tel que $\prod_{j=0}^{i} c_j = \lambda \prod_{j=0}^{i} a_j$. On déduit de (6) que r_{i+1} divise λc_{i+1}, puis que $r_{i+1}/(r_{i+1} \wedge c_{i+1})$ divise λ. On re-multiplie par $\prod_{j=0}^{i} a_j$ et on obtient :

$$\frac{r_{i+1} a_i}{r_{i+1} \wedge c_{i+1}} \prod_{j=0}^{i-1} a_j \text{ divise } \prod_{j=0}^{i} c_j \implies \frac{r_{i+1}(r_{i+1} \wedge a_i)}{r_{i+1} \wedge c_{i+1}} \prod_{j=0}^{i-1} a_j \text{ divise } \prod_{j=0}^{i} c_j \,.$$

En utilisant (5), on trouve que $r_i \prod_{j=0}^{i-1} a_j$ divise $\prod_{j=0}^{i-1} c_j$, ce qui est la propriété recherchée pour i. En fin de récurrence descendante, pour $i = 0$, on obtient que r_0 divise c_0.

Question 3.10.

On veut une procédure récursive de construction d'un hyper-rectangle latin de dimension d, de taille $\vec{c}$ compatible avec p. On commence par définir le $(d-1)$-uple $\vec{a}$ par la formule donnée dans l'énoncé juste avant la question 3.7. Puis on construit un hyper-rectangle latin de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$ en définissant une matrice A de taille $(d-1) \times d$, à partir des coefficients de $\vec{c}$ et $\vec{a}$. La construction de A est donnée ci-après. On va montrer par récurrence sur d que la construction est correcte et qu'en plus, la sous-matrice carrée droite de taille $(d-1)$ de A est toujours triangulaire inférieure avec des 1 sur la diagonale.

Commençons par le cas $d = 2$. Il suffit de considérer $\vec{c}$ élémentaire (voir les explications données dans l'énoncé entre les questions 3.5 et 3.6), c'est-à-dire $\vec{c} = (p, p)$. Ici, le $(d-1)$-uple $\vec{a}$ donné par la formule est simplement $\vec{a} = (a_0) = p$. On considère $A = (1, 1)$ ce qui correspond à l'application $T(\vec{x}) = x_0 + x_1 \bmod p$ de $\mathcal{N}_{(p,p)}$ dans $\mathcal{N}_p$ qui définit bien un carré latin comme étudié a la question 2.8.

Supposons à présent que la construction soit correcte en dimension $(d-1)$ et qu'elle fournisse toujours une matrice de taille $(d-2) \times (d-1)$ telle que la sous-matrice carrée droite de taille $(d-2)$ soit triangulaire inférieure avec des 1 sur la diagonale. Soit alors $\vec{c}$ de taille d, compatible avec p. On commence par construire (par le même principe mais en dimension $(d-1)$) un hyper-rectangle latin de taille $\underline{\vec{c}}$ compatible avec $p/(p \wedge c_{d-1})$ (d'après la première partie de la propriété (5) de la question 3.7). D'après l'hypothèse de récurrence, cette construction est correcte et définit un hyper-rectangle latin en dimension $(d-1)$ de $\mathcal{N}_{\underline{\vec{c}}}$ dans $\mathcal{N}_{\underline{\vec{a}}}$ (en effet, d'après la propriété (4) de la question 3.7, le $(d-2)$-uple construit par la formule à partir de $\underline{\vec{c}}$ est bien $\underline{\vec{a}}$) comme une application $\underline{A}_{\underline{\vec{a}}}$ où $\underline{A}$ est une matrice de taille $(d-2) \times (d-1)$. On note $\vec{u}$ la colonne d'indice 0 de $\underline{A}$ et T la sous-matrice carrée de taille $(d-2)$ définie par les autres colonnes. Par hypothèse de récurrence, la matrice T est triangulaire inférieure avec des 1 sur la diagonale.

On définit ensuite $\vec{w}$ par la récurrence descendante donnée dans l'énoncé juste avant la question 3.9. On pose $r_{d-2} = a_{d-2}$, puis pour $0 \leq i \leq d-3$, on pose :

$$w_i = \frac{r_{i+1}}{c_{i+1} \wedge r_{i+1}}, \; r_i = (a_i w_i) \wedge r_{i+1} \,.$$

Le coefficient r_{i+1} permet de définir w_i qui permet de définir r_i, etc. Puis, on définit $\vec{z}$ par les relations $z_0 = 1 - \vec{w}.\vec{u}$ et $(z_1, \dots, z_{d-2}) = -\vec{w}T$. Enfin, on définit la matrice A comme à la question 3.6 à partir de $\underline{A}$ et $\vec{z}$. La sous-matrice droite de A, de taille $(d-1) \times (d-1)$, est bien triangulaire inférieure avec des 1 sur la diagonale. Il reste à vérifier que $A_{\vec{a}}$, comme application de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$, définit bien un hyper-rectangle latin de taille $\vec{c}$. D'après la propriété (3) de la question 3.7, a_{d-2} divise c_{d-1}, donc d'après le résultat de la question 3.6 et la construction de A, il suffit de vérifier que $A_{\vec{a}}$ est une multi-bijection de $\mathcal{N}_{\vec{c}}(d-1, 0)$ dans $\mathcal{N}_{\vec{a}}$. D'après le résultat de la question 3.4, il suffit donc de vérifier que $B_{\vec{a}}$ est une multi-bijection de $\mathcal{N}_{\vec{b}}$ dans $\mathcal{N}_{\vec{a}}$ où B est la matrice obtenue en supprimant la dernière colonne de A et $\vec{b}$ est obtenu en supprimant la composante $(d-1)$ de $\vec{c}$ (en d'autres termes, $\vec{b} = \underline{\vec{c}}$). La matrice B est carrée de taille $(d-1)$, elle est en fait égale à la matrice B donnée dans l'énoncé avant cette dernière question. Elle est donc unimodulaire et $B^{-1} = EF$ avec :

$$E = \left(\begin{array}{c|c} 1 & 0 \dots 0 \\ \hline u_0 & \\ \vdots & T \\ u_{d-3} & \end{array}\right)^{-1} \quad \text{et} \quad F = \left(\begin{array}{c|c} w_0 \ \dots \ w_{d-3} & 1 \\ \hline & 0 \\ I & \vdots \\ & 0 \end{array}\right) .$$

La matrice E est triangulaire inférieure avec des 1 sur la diagonale (car T est triangulaire inférieure avec des 1 sur la diagonale) et la matrice F est unimodulaire. On va maintenant utiliser le résultat de la question 1.7 qui donne une condition suffisante pour que l'application $B_{\vec{a}}$ soit une bijection dans $\mathcal{N}_{\vec{a}}$.

Soit D la matrice diagonale telle que $D(i,i) = a_i$. Montrons que les coefficients diagonaux des formes d'Hermite de FD et EFD sont les mêmes. Soit $FD = HQ$ où H est la forme d'Hermite de FD. On a $EFD = EHQ$ et EH est triangulaire inférieure de même diagonale que H. Pour obtenir la forme d'Hermite de EFD, il suffit alors d'effectuer quelques opérations supplémentaires sur les colonnes (comme on l'a fait en fin de question 1.3), mais ceci ne change pas les coefficients diagonaux. On a :

$$E(FD) = E(HQ) = (EH)Q = (H'Q')Q = H'(Q'Q)$$

et H', forme d'Hermite de EFD, a les mêmes coefficients diagonaux que H. Il suffit donc de calculer la diagonale $\vec{h}$ de la forme d'Hermite de FD. On déduira par la question 1.7 que $B_{\vec{a}}$ est une bijection de $\mathcal{N}_{\vec{h}}$ dans $\mathcal{N}_{\vec{a}}$. On a :

$$FD = \left(\begin{array}{c|c} a_0 w_0 \ \dots \ a_{d-3} w_{d-3} & a_{d-2} \\ \hline & 0 \\ S & \vdots \\ & 0 \end{array}\right)$$

où S est la matrice diagonale de taille $(d-2)$ dont la diagonale $\vec{s}$ est égale à $\underline{\vec{a}}$. Cette matrice est du type de la matrice C de la question 3.8, matrice pour laquelle on sait calculer symboliquement la forme d'Hermite. D'après le calcul de la question 3.8, la diagonale $\vec{h}$ de la forme d'Hermite de FD est donnée par la relation suivante, pour $0 \leq i \leq d-3$, :

$$r_{d-2} = a_{d-2}, \ h_{i+1} = \frac{r_{i+1} a_i}{r_i}, \ r_i = (a_i w_i) \wedge r_{i+1} ,$$

et enfin $h_0 = r_0$. La variable intermédiaire r_{i+1} qui a permis de définir w_i est en fait la même que la variable r_{i+1} permettant de calculer les h_i. D'après le résultat de la question 3.9, on sait que pour tout $i > 0$, h_i divise c_i et que r_0 divise c_0. Puisque $h_0 = r_0$, on en déduit que $\vec{h}$ divise (composante par composante) $\vec{c}$. Enfin, puisque $B_{\vec{a}}$ est une bijection de $\mathcal{N}_{\vec{h}}$ dans $\mathcal{N}_{\vec{a}}$, $B_{\vec{a}}$ est une multi-bijection de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$ puisque $\mathcal{N}_{\vec{c}}$ est une union disjointe de translatés de $\mathcal{N}_{\vec{h}}$. Ceci termine la démonstration.

Obtenir le programme présenté en fin d'énoncé n'est pas totalement immédiat et demande plusieurs étapes d'optimisation et de fusion de boucles (ce travail n'était pas demandé).

Bilan de l'épreuve

Traiter tout le sujet dans le temps imparti n'était certainement pas réalisable. De fait, la troisième partie n'a quasiment pas été abordée par les candidats. Précisons donc que traiter parfaitement l'une des deux premières parties permettait d'obtenir une très bonne note.

Les questions 1.1 à 1.4 ont été bien résolues dans un bon nombre de copies. Les questions 1.5 à 1.8 sont beaucoup moins bien traitées. Parmi celles-ci, seule la question 1.5 était vraiment difficile. La seconde partie n'a pas été très bien traitée. De nombreux candidats ont répondu aux questions les plus abordables (2.1, 2.2, première moitié de 2.3 et 2.6) . En revanche, presque aucun n'a compris comment utiliser les groupes pour répondre aux questions difficiles, et en particulier à la question 2.4.

Notes bibliographiques

Le sujet portait sur l'utilisation des formes d'Hermite comme outil pour la génération d'hyper-rectangles latins de toute dimension et de toute taille compatible. Cette construction est issue de l'article [2] dans lequel les hyper-rectangles latins sont utilisés pour répartir des données multi-dimensionnelles sur différents processeurs, dans un souci d'équilibrage de charge. Notons qu'il est possible de construire des hyper-rectangles latins sans faire appel à la notion de forme d'Hermite en raisonnant directement sur les facteurs premiers de p. Néanmoins, la construction précédente a le mérite de conduire à une forme particulièrement condensée de génération et de description des hyper-rectangles latins.

Pour plus de détails sur les décompositions de matrices entières, on peut se référer au livre de Newman [5]. L'enchaînement des questions de la partie 1 s'inspire de l'exercice 4.1 de [3]. Les références sur les carrés latins sont nombreuses, on pourra consulter par exemple les livres de Dénes et Keedwell [4] et de Bouteloup [1]. Il est évident que seule une petite partie des résultats connus sur les carrés latins, eulériens et magiques est abordée dans ce sujet.

Remerciements

Nos sincères remerciements vont à Monsieur Mollier qui fut notre Professeur de Mathématiques, à l'un comme à l'autre, en Math. Spé. au lycée Louis-le-Grand en 1987-1988.

Références

[1] J. Bouteloup. *Carrés Magiques, Carrés Latins et Eulériens. Histoire, Théorie, Pratique.* Éditions du Choix, 1991.

[2] D. Chavarría-Miranda, A. Darte, R. Fowler, and J. Mellor-Crummey. Generalized multipartitioning for multi-dimensional arrays. In 16-*th Int. Parallel Distributed Processing Symposium (IPDPS 2002).* IEEE Computer Society Press, 2002.

[3] A. Darte and S. Vaudenay. *Algorithmique et optimisation : exercices corrigés.* Sciences Sup. Dunod, 2001.

[4] J. Dénes and A. D. Keedwell. *Latin Squares : New Developments in the Theory and Applications.* North Holland, 1991.

[5] M. Newman. *Integral Matrices.* Academic Press, 1972.