UL 220 J. 2035

SESSION 2002

Filières MP et PC (groupe I)

(Epreuve commune aux ENS de Paris et Lyon)

MATHEMATIQUES-INFORMATIQUE

Durée : 4 heures

L'usage de toute calculatrice est interdit.

Tournez la page S.V.P.

Autour des carrés latins

Notations

On note $\mathbb{N}$ l'ensemble des entiers naturels, $\mathbb{Z}$ l'ensemble des entiers relatifs, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ et, pour tout $n \in \mathbb{N}^*$, $\mathcal{N}_n$ l'ensemble des entiers de 0 à $n-1$. Si $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, on note $p \div q$ et $p \bmod q$ le quotient et le reste dans la division euclidienne de p par q, c'est-à-dire les uniques entiers tels que $0 \leq p \bmod q < q$ et $q(p \div q) + (p \bmod q) = p$. Si $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$, on note $p \wedge q$ le plus grand diviseur commun (**pgcd**) de p et de q lorsque $(p,q) \neq (0,0)$ et, par convention, $0 \wedge 0 = 0$. Par définition, le pgcd est donc un entier strictement positif sauf si $(p,q) = (0,0)$. On définit de façon similaire le pgcd d'un ensemble d'entiers. On rappelle que, pour $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$, les quatre propriétés suivantes sont équivalentes : (i) $p \wedge q = 1$, (ii) il existe $(u,v) \in \mathbb{Z}^2$ tel que $pu + qv = 1$ (propriété de Bezout), (iii) $\exists u \in \mathbb{Z}$ tel que $pu \bmod q = 1$, (iv) $p \bmod q$ est un générateur du groupe défini par $\mathcal{N}_q$ muni de l'addition modulo q.

Une matrice A de taille $n \times m$ à coefficients dans S est une famille $[A(i,j)]_{(i,j) \in \mathcal{N}_n \times \mathcal{N}_m}$ d'éléments de S. Une matrice carrée de taille n est une matrice de taille $n \times n$. La ligne d'indice i (resp. la colonne d'indice j) de A est la famille $[A(i,j)]_{j \in \mathcal{N}_m}$ (resp. $[A(i,j)]_{i \in \mathcal{N}_n}$). Attention : les lignes et colonnes sont donc indexées à partir de 0 et non à partir de 1, ceci pour simplifier les notations de certaines parties du sujet. De même, on numérote les composantes d'un n-uple $\vec{x} \in \mathbb{Z}^n$ de 0 à $(n-1)$ et on note x_i sa composante d'indice i.

Partie 1. Quelques propriétés des matrices carrées entières

Une matrice est **entière** si elle est à coefficients dans $\mathbb{Z}$. On dit qu'une matrice est **unimodulaire** si elle est carrée, entière et si son déterminant vaut 1 ou -1. Avec l'addition et le produit usuels sur les matrices, l'ensemble des matrices entières carrées de taille n forme un anneau $\mathcal{M}_n(\mathbb{Z})$ dont l'élément unité est noté I.

Forme d'Hermite d'une matrice carrée entière

On note $E_{i,j}$ la matrice dont tous les coefficients sont nuls sauf $E_{i,j}(i,j) = 1$. Les matrices $P_{i,j} = I - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$, $S_i = I - 2E_{i,i}$ et, lorsque $i \neq j$, $R_{i,j} = I - E_{i,j}$ sont appelées matrices **élémentaires**.

Question 1.1. *Quel est l'effet, sur une matrice $A \in \mathcal{M}_n(\mathbb{Z})$, de la multiplication à droite par une matrice élémentaire ? Quel est le déterminant des matrices élémentaires ? Ont-elles un inverse dans $\mathcal{M}_n(\mathbb{Z})$?*

Question 1.2. *Que fait l'algorithme de la figure 1 pour une matrice $A \in \mathcal{M}_n(\mathbb{Z})$? Montrer qu'il se termine toujours et que, quel que soit i, le pgcd de la ligne d'indice i de A n'est pas modifié par l'algorithme.*

Question 1.3. *Soit $A \in \mathcal{M}_n(\mathbb{Z})$. Montrer, en donnant un algorithme inspiré de celui de la question précédente, qu'il existe une matrice $H \in \mathcal{M}_n(\mathbb{Z})$ triangulaire inférieure, à diagonale positive ou nulle, et une matrice unimodulaire Q telles que $A = HQ$. Montrer que si le déterminant de A est non nul, on peut de plus imposer $0 \leq H(i,j) < H(i,i)$ pour tout $j < i$.*

Pour j **de** 0 **à** $n-1$
  Si $(A(0,j) < 0)$ $A \leftarrow AS_j$;
FinPour
$C \leftarrow \{j \in \mathcal{N}_n \mid A(0,j) \neq 0\}$;
Tant que $(C \neq \emptyset)$
  $m \leftarrow \min\{A(0,j) \mid j \in C\}$;
  Soit $k \in C$ tel que $A(0,k) = m$;
  $A \leftarrow AP_{0,k}$;
  Pour j **de** 1 **à** $n-1$
    $q \leftarrow A(0,j) \div m$;
    $A \leftarrow A(R_{0,j})^q$;
  FinPour
  $C \leftarrow \{j \in \mathcal{N}_n \backslash \{0\} \mid A(0,j) \neq 0\}$;
FinTantQue

FIG. 1 – Algorithme de la question 1.2.

Question 1.4. *Montrer que toute matrice unimodulaire est produit de matrices élémentaires et que l'ensemble des matrices unimodulaires de taille n est l'ensemble des inversibles de* $\mathcal{M}_n(\mathbb{Z})$.

Question 1.5. *Montrer que si le déterminant de* A *est non nul, il existe une unique décomposition* $A = HQ$ *vérifiant toutes les propriétés de la question 1.3. On dit alors que la matrice* H *est* **la forme d'Hermite** *de* A.

Équations en nombres entiers et opérations « modulo »

Étant donné un n-uple $\vec{a} \in (\mathbb{N}^*)^n$, on note $\mathcal{N}_{\vec{a}} = \{\vec{x} \in \mathbb{Z}^n \mid \forall i,\ 0 \leq x_i < a_i\}$. Si $A \in \mathcal{M}_n(\mathbb{Z})$, on définit l'application $A_{\vec{a}} : \mathbb{Z}^n \to \mathcal{N}_{\vec{a}}$ par $A_{\vec{a}}(\vec{x}) = (A\vec{x}) \bmod \vec{a}$ où l'opération modulo est calculée composante par composante, c'est-à-dire $\forall i$, $(A_{\vec{a}}(\vec{x}))_i = (A\vec{x})_i \bmod a_i$. Dans la suite, on suppose que $A \in \mathcal{M}_n(\mathbb{Z})$ et $\vec{a} \in (\mathbb{N}^*)^n$ sont donnés et on cherche des conditions pour que la restriction de $A_{\vec{a}}$ à un ensemble de la forme $\mathcal{N}_{\vec{c}}$ soit une bijection de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$. On note $\vec{0} = (0, \ldots, 0)$.

Question 1.6. *Soit* $\vec{c} \in (\mathbb{N}^*)^n$. *Montrer que la restriction de* $A_{\vec{a}}$ *à* $\mathcal{N}_{\vec{c}}$ *est injective si et seulement si* $\vec{0}$ *est l'unique solution de* $A\vec{x} \bmod \vec{a} = \vec{0}$ *avec* $\vec{x} \in \mathbb{Z}^n$ *et* $\forall i$, $-c_i < x_i < c_i$.

On note $D = \mathrm{diag}(\vec{a})$ la matrice de $\mathcal{M}_n(\mathbb{Z})$, diagonale, définie par $\forall i$, $D(i,i) = a_i$. On vérifie alors aisément que $A\vec{x} \bmod \vec{a} = \vec{0}$ si et seulement s'il existe $\vec{y} \in \mathbb{Z}^n$ tel que $A\vec{x} = D\vec{y}$.

Question 1.7. *On suppose pour commencer que* $\vec{c}$ *et* $\vec{a}$ *sont quelconques dans* $(\mathbb{N}^*)^n$ *mais que* A *est unimodulaire. Montrer que si la diagonale de la forme d'Hermite de* $A^{-1}D$ *est égale à* $\vec{c}$ *alors la restriction de* $A_{\vec{a}}$ *à* $\mathcal{N}_{\vec{c}}$ *est une bijection de* $\mathcal{N}_{\vec{c}}$ *dans* $\mathcal{N}_{\vec{a}}$.

Question 1.8. *On suppose à présent que* A *est quelconque mais que* $\vec{c} = \vec{a} = (a, \ldots, a)$. *On a alors* $D = aI$. *En utilisant la forme d'Hermite de* A, *montrer que si* $\det(A) \wedge a = 1$ *alors la restriction de* $A_{\vec{a}}$ *à* $\mathcal{N}_{\vec{c}}$ *est injective. Montrer que si* $A_{\vec{a}}$ *est surjective, il existe deux matrices* $B \in \mathcal{M}_n(\mathbb{Z})$ *et* $C \in \mathcal{M}_n(\mathbb{Z})$ *telles* $AB = I + aC$. *En déduire que* $\det(A) \wedge a = 1$. *Conclure.*

Partie 2. Quelques propriétés des carrés latins

Carrés latins et groupes

On dit qu'une matrice carrée de taille n à coefficients dans $\mathcal{N}_n$ est un **carré latin** de taille n si chaque élément de $\mathcal{N}_n$ apparaît exactement une fois dans chaque ligne et dans chaque colonne. On dit que deux carrés latins A et B sont **équivalents** si on peut passer de l'un à l'autre par renommage bijectif des éléments et permutation des lignes et des colonnes, c'est-à-dire si A et B sont de même taille n et s'il existe trois permutations f, g et h de $\mathcal{N}_n$ telles que pour tout $(i,j) \in \mathcal{N}_n \times \mathcal{N}_n$, $B(i,j) = f(A(g(i),h(j)))$. Cette relation sur les carrés latins est évidemment une relation d'équivalence.

Un ensemble muni d'une loi de composition interne est appelé **magma**. À un carré latin A de taille n, on **associe** le magma $(\mathcal{N}_n, \star)$ où la loi $\star$ est donnée par $x \star y = A(x,y)$.

Question 2.1. *Construire un carré latin dont le magma associé n'a pas d'élément neutre. Montrer que pour tout carré latin, il existe un carré latin équivalent dont le magma associé possède 0 comme élément neutre. Combien y a-t-il de classes d'équivalence de carrés latins de taille n pour $n \leq 3$? De carrés latins de taille n pour $n \leq 3$?*

Question 2.2. *Existe-t-il des carrés latins de n'importe quelle taille ?*

Question 2.3. *Soit $(G, \bullet)$ un magma possédant un élément neutre et soit $(H, \star)$ un magma dont la loi $\star$ est associative. On suppose qu'il existe une bijection f de G dans H et deux bijections g et h de H dans G telles que pour tout $(x,y) \in H \times H$, $x \star y = f(g(x) \bullet h(y))$. Montrer que pour tout $(x,y,z) \in H \times H \times H$, $g(f(g(x) \bullet h(y))) \bullet h(z) = g(x) \bullet h(f(g(y) \bullet h(z)))$. En déduire que $hfg = gfh$, puis montrer que hfg est un isomorphisme, c'est-à-dire que pour tout $(x,y) \in H \times H$, $hfg(x \star y) = hfg(x) \bullet hfg(y)$.*

Question 2.4. *Donner un représentant par classe d'équivalence de carrés latins de taille 4. Construire un carré latin de taille minimale qui ne soit pas équivalent à un carré latin associé à un groupe. Dans les deux cas, ne pas oublier de justifier avec soin.*

Carrés eulériens et carrés magiques

Étant donnés deux carrés latins A et B de taille n, on définit la matrice $C = (A, B)$ à coefficients dans $\mathcal{N}_n \times \mathcal{N}_n$ par $C(i,j) = (A(i,j), B(i,j))$. Si tous les coefficients de C sont distincts, on dit que A et B sont **orthogonaux** et que C est un **carré eulérien** de taille n.

Question 2.5. *Soient A et B deux carrés latins de taille n. Pour tout $j \in \mathcal{N}_n$, on note σ_j la permutation telle que, pour tout i, $B(i, \sigma_j(i)) = j$. Montrer que A et B sont orthogonaux si et seulement si, quel que soit j, tous les $A(i, \sigma_j(i))$ sont distincts. En déduire qu'un carré latin associé à un groupe cyclique d'ordre pair n'a pas d'orthogonal. (On pourra considérer la somme, modulo $2p$, de tous les éléments de $\mathcal{N}_{2p}$.)*

Un carré latin de taille n est **diagonal** si tous les éléments $A(i,i)$ de la diagonale sont distincts, ainsi que tous les éléments $A(i, n-1-i)$ de l'anti-diagonale. Un carré eulérien (A, B) est diagonal si A et B sont diagonaux. Une matrice carrée de taille n, à coefficients dans $\mathcal{N}_{n^2}$, est un **carré magique** de taille n si tous ses coefficients sont distincts et si toutes les sommes des coefficients d'une ligne, d'une colonne, de la diagonale et de l'anti-diagonale sont égales ($\exists k \in \mathbb{N}$, $\forall i$, $\sum_j A(i,j) = k$, $\forall j$, $\sum_i A(i,j) = k$ et $\sum_i A(i,i) = \sum_i A(i, n-i-1) = k$).

Question 2.6. *Montrer que l'on peut construire un carré magique de taille n à partir d'un carré eulérien diagonal de taille n.*

Question 2.7. *Pour $n \leq 4$, déterminer s'il existe des carrés eulériens, des carrés eulériens diagonaux et des carrés magiques de taille n. En cas de réponse positive, en donner un exemple.*

Question 2.8. *Donner une condition nécessaire et suffisante sur $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ pour que la matrice de taille n définie par $A(i,j) = (ai + bj) \bmod n$ soit un carré latin. Même question pour un carré latin diagonal. Soient a, b, c, d dans $\mathbb{Z}$. Montrer que les deux carrés latins définis par $A(i,j) = (ai + bj) \bmod n$ et $B(i,j) = (ci + dj) \bmod n$ sont orthogonaux si et seulement si $(ad - bc) \wedge n = 1$. (On pourra raisonner directement en introduisant $u \in \mathcal{N}_n$ tel que $(c + du) \bmod n = 0$ ou bien faire le lien avec la question 1.8.)*

Question 2.9. *Montrer qu'il existe un carré magique de taille n pour tout entier n qui n'est multiple ni de 2 ni de 3. Donner un carré magique de taille 5.*

Partie 3. Hyper-rectangles latins

On dit qu'une application f de E dans F définit une **multi-bijection** de E' dans F, pour $E' \subset E$, si tous les éléments de F ont le même nombre d'antécédents par f dans E'. Un **tableau** de dimension $d \in \mathbb{N}$, $d \geq 2$, de taille $\vec{c} \in (\mathbb{N}^*)^d$, dans un ensemble S, est une application de $\mathcal{N}_{\vec{c}}$ dans S. Un tableau T est un **hyper-rectangle latin** si $\forall i$, $0 \leq i < d$, $\forall k$, $0 \leq k < c_i$, l'application T définit une multi-bijection de $\mathcal{N}_{\vec{c}}(i,k) = \{\vec{x} \in \mathcal{N}_{\vec{c}} \mid x_i = k\}$ dans S. Autrement dit, un tableau peut être vu comme la généralisation d'une matrice en dimension d et un tableau est un hyper-rectangle latin si dans tout sous-tableau obtenu en fixant un indice, tous les éléments de S apparaissent le même nombre de fois. Lorsque toutes les multi-bijections sont des bijections (chaque élément apparaît alors une et une seule fois dans chacun des sous-tableaux), on dit que le tableau est un **hyper-cube latin**. En dimension 2, lorsque $S = \mathcal{N}_p$, les hyper-cubes latins sont de taille $\vec{c} = (p,p)$ et on retrouve la notion de carré latin de taille p.

Étude des tailles compatibles élémentaires

On s'intéresse pour commencer au problème suivant : comment répartir n boules identiques dans d boîtes distinctes de sorte que chaque boîte contienne au plus m boules et qu'au moins c boîtes en contiennent exactement m.

Question 3.1. *Montrer qu'il existe une telle répartition si et seulement si $0 \leq c \leq d$ et $cm \leq n \leq dm$. Expliquer, en justifiant avec précision, ce que fait la procédure $P(n, m, c, d)$ de la figure 2 lorsque $d \geq 1$, $0 \leq c \leq d$ et $cm \leq n \leq dm$. (Par convention, une boucle « **Pour** i **de** u **à** v » n'est pas exécutée si $v < u$.)*

Pour qu'il existe un hyper-rectangle latin de taille $\vec{c}$, de dimension d, dans un ensemble de cardinal p, il faut évidemment que, pour tout i, $\prod_{j \neq i} c_j$ soit un multiple de p. Lorsque $\vec{c}$ vérifie cette propriété, on dit que $\vec{c}$ est une taille **compatible** avec p. Lorsque, de plus, il n'existe pas de taille $\vec{b} \neq \vec{c}$, compatible avec p, telle que $\forall i$, $c_i = k_i b_i$ avec $k_i \in \mathbb{N}^*$, on dit que $\vec{c}$ est **élémentaire** pour p. L'objet des questions suivantes est de générer toutes les tailles élémentaires pour p.

Étant donnés u et v dans $\mathbb{N}^*$, on définit l'**occurrence** de v dans u comme le plus grand entier naturel r tel que v^r divise u.

Tournez la page S.V.P.

```
P(n, m, c, d) {
   Si (d = 1)
      boîte[d − 1] = n ;
   Sinon
      Pour i de max(0, n − m(d − 1)) à min(m − 1, n − cm)
         boîte[d − 1] = i ;
         P(n − i, m, c, d − 1) ;
      FinPour
      Si (n ≥ m)
         boîte[d − 1] = m ;
         P(n − m, m, max(0, c − 1), d − 1) ;
      FinSi
   FinSi
}
```

FIG. 2 – Code de la procédure P.

Question 3.2. *Soit $\vec{c}$ une taille compatible avec p et α un facteur premier de p d'occurrence r. On note m l'occurrence maximale de α dans une composante de $\vec{c}$. Montrer que l'occurrence de α dans $\prod_i c_i$ est au moins $r + m$. Montrer de plus que si $\vec{c}$ est élémentaire pour p, alors l'occurrence de α est égale à m pour au moins deux composantes de $\vec{c}$ et l'occurrence de α dans $\prod_i c_i$ est exactement $r + m$.*

Question 3.3. *Lorsque p n'a qu'un seul facteur premier, écrire un programme utilisant la procédure P de la figure 2 pour générer toutes les tailles élémentaires pour p. Comment pourrait-on générer toutes les tailles élémentaires pour un entier p quelconque ?*

Une construction particulière d'hyper-rectangles latins de la forme $A_{\vec{a}}$

Soient $p \in \mathbb{N}^*$, $d \geq 2$ et $\vec{c} \in (\mathbb{N}^*)^d$, compatible avec p. L'objet de cette dernière partie est de mettre au point un programme compact, généralisant le principe de construction d'un carré latin de la question 2.8, pour construire $\vec{a} \in (\mathbb{N}^*)^{d-1}$ (avec $\prod_i a_i = p$) et une matrice entière A, de taille $(d-1) \times d$, tels que l'application $A_{\vec{a}}$ de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$, définie par $A_{\vec{a}}(\vec{x}) = (A\vec{x}) \bmod \vec{a}$, soit un hyper-rectangle latin.

Question 3.4. *Soient $\vec{a} \in (\mathbb{N}^*)^{d-1}$ et A entière de taille $(d-1) \times d$. Montrer que les propriétés suivantes sont équivalentes : (i) $A_{\vec{a}}$ est un hyper-rectangle latin de $\mathcal{N}_{\vec{c}}$ dans $\mathcal{N}_{\vec{a}}$, (ii) $\forall i$, $0 \leq i < d$, $A_{\vec{a}}$ définit une multi-bijection de $\mathcal{N}_{\vec{c}}(i, 0)$ dans $\mathcal{N}_{\vec{a}}$, (iii) $\forall i$, $0 \leq i < d$, $B_{\vec{a}}$ définit une multi-bijection de $\mathcal{N}_{\vec{b}}$ dans $\mathcal{N}_{\vec{a}}$ où $B \in \mathcal{M}_{d-1}(\mathbb{Z})$ est la matrice obtenue en supprimant la colonne d'indice i de A et $\vec{b} \in (\mathbb{N}^*)^{d-1}$ est obtenu en supprimant la composante d'indice i de $\vec{c}$.*

Question 3.5. *On s'intéresse ici au cas particulier des hyper-cubes. Vérifier que s'il existe un hyper-cube latin de taille $\vec{c}$ alors $p = q^{d-1}$ avec $q \in \mathbb{N}^*$ et $\vec{c} = (q, \ldots, q)$ (d'où l'appellation de « cube »). Réciproquement, lorsque $p = q^{d-1}$ et $\vec{c} = (q, \ldots, q)$ avec $q \in \mathbb{N}^*$, construire un hyper-cube latin de taille $\vec{c}$ dans un ensemble de cardinal p. (On pourra s'inspirer des résultats des questions 1.8 et 3.4 et choisir une matrice bi-diagonale.)*

Si $A_{\vec a}$ définit un hyper-rectangle latin de $\mathcal{N}_{\vec b}$ dans $\mathcal{N}_{\vec a}$ et si $\vec c$ vérifie $\forall i,\ c_i = k_i b_i$ avec $k_i \in \mathbb{N}^*$, alors $A_{\vec a}$, en tant qu'application de $\mathcal{N}_{\vec c}$ dans $\mathcal{N}_{\vec a}$, définit également un hyper-rectangle latin. Il suffit donc de savoir construire un hyper-rectangle latin de n'importe quelle taille élémentaire pour savoir construire un hyper-rectangle latin de n'importe quelle taille compatible. En dimension 2, il n'existe qu'une taille élémentaire pour p, c'est (p,p) qui correspond à un carré latin de taille p. En dimension $d \geq 3$ en revanche, toutes les tailles élémentaires ne correspondent pas à des hyper-cubes latins (considérer par exemple $(15,10,6)$ qui est élémentaire pour 30) et il ne suffit pas de savoir construire des hyper-cubes latins pour savoir construire des hyper-rectangles latins de n'importe quelle taille compatible. L'objet des questions suivantes est de mettre en place un procédé différent de construction d'hyper-rectangles latins, par récurrence sur la dimension.

Dans la suite, pour un n-uple $\vec x$, on note $\underline{\vec x}$ le $(n-1)$-uple obtenu en supprimant la dernière composante de $\vec x$.

Question 3.6. *Soient $\vec a \in (\mathbb{N}^*)^{d-1}$ et $\underline{A}$ une matrice entière de taille $(d-2)\times(d-1)$ telle que $\underline{A}_{\underline{\vec a}}$ soit un hyper-rectangle latin de dimension $(d-1)$ de $\mathcal{N}_{\underline{\vec c}}$ dans $\mathcal{N}_{\underline{\vec a}}$. Soit A une matrice entière de taille $(d-1)\times d$ de la forme :*

$$A = \left(\begin{array}{ccc|c} & & & 0 \\ & \underline{A} & & \vdots \\ & & & 0 \\ \hline z_0 & \cdots & z_{d-2} & 1 \end{array}\right)$$

Montrer que si la dernière composante de $\vec a$ (c'est-à-dire a_{d-2}) divise la dernière composante de $\vec c$ (c'est-à-dire c_{d-1}) et que $A_{\vec a}$ est une multi-bijection de $\mathcal{N}_{\vec c}(d-1,0)$ dans $\mathcal{N}_{\vec a}$ alors $A_{\vec a}$ est un hyper-rectangle latin de dimension d de $\mathcal{N}_{\vec c}$ dans $\mathcal{N}_{\vec a}$.

On définit à présent $\vec a$, en fonction de $\vec c$ et p, par la formule suivante (où, par convention, un produit sans termes vaut 1) :

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

Question 3.7. *Montrer que, pour des entiers u, v et w non nuls, on a $u \wedge (vw) = (u \wedge v)(\frac{u}{u\wedge v} \wedge w)$. Montrer les propriétés suivantes : (1) $\vec a \in (\mathbb{N}^*)^{d-1}$, (2) $\prod_{i=0}^{d-2} a_i = p$, (3) $\forall i,\ 0 \leq i \leq d-2$, a_i divise c_{i+1}, (4) on retrouve $\underline{\vec a}$ en appliquant la formule (1) avec $\underline{\vec c}$ et l'entier $\frac{p}{p\wedge c_{d-1}}$, (5) $\underline{\vec c}$ est compatible avec $\frac{p}{p\wedge c_{d-1}}$ et, $\forall i,\ 0 \leq i \leq d-2$, $\prod_{j=0}^{i} c_j$ est multiple de $\prod_{j=0}^{i} a_j$.*

Question 3.8. *Soit $S = \mathrm{diag}(\vec s)$, matrice diagonale de $\mathcal{M}_{d-2}(\mathbb{Z})$, et $C \in \mathcal{M}_{d-1}(\mathbb{Z})$ de la forme :*

$$C = \left(\begin{array}{ccc|c} v_0 & \cdots & v_{d-3} & v_{d-2} \\ \hline & & & 0 \\ & S & & \vdots \\ & & & 0 \end{array}\right)$$

En considérant pour commencer le cas où C est de taille 2 puis en généralisant, montrer que la diagonale $\vec h \in (\mathbb{N}^*)^n$ de la forme d'Hermite de C est donnée par la récurrence descendante suivante : $r_{d-2} = v_{d-2}$, $h_{i+1} = \frac{r_{i+1} s_i}{r_i}$ et $r_i = v_i \wedge r_{i+1}$ pour $0 \leq i \leq d-3$, enfin $h_0 = r_0$.

On étudie maintenant la récurrence descendante définie par $r_{d-2} = a_{d-2}$ et, pour $0 \leq i \leq d-3$, $w_i = \frac{r_{i+1}}{c_{i+1} \wedge r_{i+1}}$, $r_i = a_i w_i \wedge r_{i+1}$ et $h_{i+1} = \frac{r_{i+1} a_i}{r_i}$.

Question 3.9. *Montrer, en utilisant la propriété (3) de la question 3.7, que* $r_i = r_{i+1}\left(\frac{r_{i+1} \wedge a_i}{r_{i+1} \wedge c_{i+1}}\right)$ *et que* h_{i+1} *divise* c_{i+1}*, lorsque* $0 \leq i \leq d-3$*. Montrer, par une récurrence descendante sur* i *et en utilisant la propriété (5) de la question 3.7, que* $r_i \prod_{j=0}^{i-1} a_j$ *divise* $\prod_{j=0}^{i} c_j$*. En déduire que* r_0 *divise* c_0*.*

Soit $T \in \mathcal{M}_{d-2}(\mathbb{Z})$, unimodulaire, et $B \in \mathcal{M}_{d-1}(\mathbb{Z})$ de la forme :

$$B = \left(\begin{array}{c|c} u_0 & \\ \vdots & T \\ u_{d-3} & \\ \hline z_0 & z_1 \ \dots \ z_{d-2} \end{array}\right)$$

On vérifie aisément que si $z_0 = 1 - \vec{w}.\vec{u} = 1 - \sum_i w_i u_i$ et $(z_1, \dots, z_{d-2}) = -\vec{w}T$ alors B est unimodulaire et son inverse est :

$$B^{-1} = \left(\begin{array}{c|c} 1 & 0 \dots 0 \\ \hline u_0 & \\ \vdots & T \\ u_{d-3} & \end{array}\right)^{-1} \left(\begin{array}{c|c} w_0 \ \cdots \ w_{d-3} & 1 \\ \hline & 0 \\ I & \vdots \\ & 0 \end{array}\right)$$

Question 3.10. *En regroupant tous les résultats de cette dernière partie et en utilisant le résultat de la question 1.7, donner un procédé récursif de construction d'un hyper-rectangle latin de toute taille* $\vec{c} \in (\mathbb{N}^*)^d$ *compatible avec* p*. (On remarquera que la matrice* T *apparaissant dans la construction est unimodulaire triangulaire inférieure et que multiplier une matrice à gauche par une matrice unimodulaire triangulaire inférieure ne change par les coefficients diagonaux de sa forme d'Hermite.)*

On peut vérifier que le programme ci-dessous suit le principe développé dans cette partie et calcule bien une matrice A telle que $A_{\vec{a}}$ soit un hyper-rectangle latin de taille $\vec{c}$ compatible avec p lorsque $\vec{a}$ est donné par la formule (1).

Matrice(d, $\vec{c}$, $\vec{a}$) {
  Pour i **de** 0 **à** $d-2$
    Pour j **de** 0 **à** $d-1$
      Si $(j = 0$ ou $j = i+1)$ $A(i,j) = 1$; **Sinon** $A(i,j) = 0$;
    FinPour
  FinPour
  Pour i **de** 1 **à** $d-2$
    $r = a_i$;
    Pour j **de** $i-1$ **à** 0 (par valeurs descendantes)
      $w = \frac{r}{r \wedge c_{j+1}}$; $r = (w\, a_j) \wedge r$;
      Pour k **de** 0 **à** i
        $A(i,k) = A(i,k) - wA(j,k)$;
      FinPour
    FinPour
  FinPour
}