Cinémath

Aurore Schneiders, Alexandre Lebailly, François Philippart de Foy,
Julien Heine, Thomas Demortier, Thibault Lowette et Simon Lemal
avec l'aide de Romain Schietaert et Xavier Heeren

2016 - 2017

Cinémath

1 Présentation du problème

1.1 Énoncé

Un groupe de n écoles souhaite se rassembler pour visionner un film. Chaque école contient n types de classe différents et propose à un seul étudiant de chaque type de classes de participer à l'évènement. La salle de cinéma contient n rangées de n sièges. Est-il possible de placer les $n \times n$ étudiants dans la salle de cinéma de sorte que chaque étudiant y soit et que, sur chaque rangée et chaque colonne de sièges, on ne retrouve ni deux écoles identiques, ni deux types de classe identiques ?

1.2 Formalisation

1.2.1 Comment désigner un élève, un siège ?

Nous avons décidé d'associer à chaque élève un couple d'entier : le premier détermine son école et le deuxième le type de classes dans laquelle il est (par convention, on commence à compter à 0). On doit ensuite placer ces élèves dans une salle de cinéma de manière à respecter les critères de l'énoncé. Cependant, chaque siège (chaque case du tableau) peut également être désigné par un couple de deux nombres, sa rangée et son numéro. Il est à noter que les nombres formant ces couples, aussi bien ceux désignant un siège que ceux désignant un élève, sont compris entre 0 et $n-1$.

On remarque alors que le problème revient à associer à chaque couple (a, b) de l'ensemble [1] $(\mathbb{Z}_n)^2$, désignant un siège, un couple du même ensemble désignant un élève (c, d), ou à trouver un fonction

$$f_n : (\mathbb{Z}_n)^2 \to (\mathbb{Z}_n)^2, (a, b) \mapsto (c, d) \tag{1}$$

répondant à certaines condition que nous allons expliquer ci-dessous. Cette fonction va en faite associer à chaque siège de la rangée a et dont le numéro est b un élève de l'école c dans le type de classe d.

1.2.2 Première condition

La première condition n'est pas formulée explicitement dans l'énoncé. On sait cependant que « Un seul étudiant de chaque classe participe à l'évenement ». Cela signifie que chaque couple (c, d) se retrouve exactement une fois, ou que la fonction f_n est bijective [2]. Chaque siège ne se voit attribuer qu'un élève, et vice-versa. Ainsi, pour chaque élève (c, d), il existe un siège (a, b), et sur deux siège différents, on trouve deux élèves différents. Pour prouver que la fonction est bijective, on prouvera

$$\forall (c, d) \in (\mathbb{Z}_n)^2,\ \exists (a, b)\ (\mathbb{Z}_n)^2 \mid f_n(a, b) = (c, d) \tag{2}$$

et

$$\forall (a, b), (a', b') \in (\mathbb{Z}_n)^2,\ f_n(a, b) = f_n(a', b') \Rightarrow (a, b) = (a', b') \tag{3}$$

qui est équivalent sa contraposée $(a, b) \neq (a', b') \Rightarrow f_n(a, b) \neq f_n(a', b')$.

Remarque. Lorsque l'on travaille avec des fonctions à ensembles domaine et image de taille finie et identique, une fonction injective est surjective et vice versa. On ne doit donc pas prouver que la fonction est injective et surjective mais seulement un des deux.
En effet, si elle est surjective, on peut en déduire que pour que chaque image soit atteinte (ce qui est la définition de la surjectivité), chaque antécédent doit avoir une image différente des autres.
Si elle est injective, chaque antécédant a une image différente des autres, donc il y a autant d'images atteintes que d'antécédents. Comme on sait que le nombre d'images est égal à celui d'antécédents, on en conclut que toutes les images sont atteintes.

1. $(\mathbb{Z}_n)^2$ peut être interpreté comme « l'ensemble des couples d'entier modulo n ». (confer sous section 5.1)
2. Cette notion est définie dans l'annexe, sous-section 5.2

1.2.3 Deuxième condition

La deuxième veut que chaque colonne et chaque ligne, chaque école et chaque type de classes soit représenté une fois. Si l'on définit

$$g, h : (\mathbb{Z}_n)^2 \to \mathbb{Z}_n \mid f_n(a, b) = (g(a, b), h(a, b)) \tag{4}$$

alors, en gardant a ou b fixé, les fonctions $g_a(b), g_b(a), h_a(b), h_b(a)$ sont toutes bijectives (la fonction $g_a(b)$ vaut $g(a, b)$, mais a est gardé constant). Le fait de fixer a ou b permet de rester sur une même ligne ou colonne, et la bijectivité des fonctions assurent que sur cette rangée, chaque premier élément (donné par g, le numéro de l'école) soit présent exactement une fois, et de même pour le deuxième élément (donné par h, le type de la classe).

2 Cas particuliers

Lorsque n est impair, le problème est facilement solvable. Il est en effet peu compliqué de trouver une configuration qui conviennent. Il en existe en fait énormément.

2.1 Exemple

Par exemple, on peut générer un premier tableau en associant à la case (a, b) sa « distance » (en terme de déplacements horizontaux et verticaux uniquement), modulo n. En associant ce tableau à son symétrique orthogonal d'axe vertical (i.e. pour la case de coordonnées (a, b), on forme un couple en prenant la valeur de la case correspondante du premier tableau comme première valeur du couple et celle du deuxième tableau comme deuxième valeur), on obtient un tableau, contenant des couples, cette fois, qui est solution du problème.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

4	3	2	1	0
0	4	3	2	1
1	0	4	3	2
2	1	0	4	3
3	2	1	0	4

TABLE 1 – *À gauche :* le premier tableau. *À droite :* son symétrique.

(0, 4)	(1, 3)	(2, 2)	(3, 1)	(4, 0)
(1, 0)	(2, 4)	(3, 3)	(4, 2)	(0, 1)
(2, 1)	(3, 0)	(4, 4)	(0, 3)	(1, 2)
(3, 2)	(4, 1)	(0, 0)	(1, 4)	(2, 3)
(4, 3)	(0, 2)	(1, 1)	(2, 0)	(3, 4)

TABLE 2 – L'association des deux tableaux.

Pourquoi est-elle solution ?

Chaque case du premier tableau est définie par sa distance à la case en haut à gauche, le tout modulo n, ce qui peut aussi bien s'exprimer $a + b$ (pour la case (a, b)). Pour le deuxième tableau, il faut penser à ce que signifie une « symétrie d'axe vertical ». En fait, cela revient à associer à la case (a, b) du deuxième tableau la case $(a, n - 1 - b)$ du premier. Ainsi, le deuxième tableau est défini par $a + (n - 1 - b) \mod n = a - b - 1 \mod n$.

Leur association est définie par $f_n(a, b) = (a + b \mod n, a - b - 1 \mod n)$. Néanmoins, on préférera démontrer que $f_n(a, b) = (a + b \mod n, a - b \mod n)$ respecte les conditions. En effet, si cette dernière fonction respecte les conditions, sa composée avec $l(a, b) = (a, b - 1 \mod n)$, i.e. la fonction $f_n(a, b) = (a+b \mod n, a-b-1 \mod n)$, les respecte aussi (car $l(a, b) = (a, b-1 \mod n)$ est bijective et la composé de deux fonctions bijectives l'est aussi).

Il reste à prouver, de manière formelle, que

$$f_n(a, b) = (a + b \mod n, a - b \mod n) \tag{5}$$

respecte la première et la deuxième condition.

(0, 0)	(1, 4)	(2, 3)	(3, 2)	(4, 1)
(1, 1)	(2, 0)	(3, 4)	(4, 3)	(0, 2)
(2, 2)	(3, 1)	(4, 0)	(0, 4)	(1, 3)
(3, 3)	(4, 2)	(0, 1)	(1, 0)	(2, 4)
(4, 4)	(0, 3)	(1, 2)	(2, 1)	(3, 0)

TABLE 3 – Le tableau généré par la nouvelle fonction.

Intuitivement, cette fonction semble convenir puisque ce tableau respecte les conditions définies dans la section 1.2.

2.2 Première condition

Proposition 2.1. *La fonction* $f_n : (\mathbb{Z}_n)^2 \to (\mathbb{Z}_n)^2, (a, b) \mapsto (a+b \mod n, a-b \mod n)$ *est injective.*

Démonstration. Supposons $f_n(a, b) = f_n(a', b') \Leftrightarrow (a+b \mod n, a-b \mod n) = (a'+b' \mod n, a'-b' \mod n)$.
C'est équivalent à

$$\begin{cases} a+b & \equiv a'+b' \pmod n \\ a-b & \equiv a'-b' \pmod n \end{cases} \Leftrightarrow \begin{cases} 2a & \equiv 2a' \pmod n \\ 2b & \equiv 2b' \pmod n \end{cases}.$$

Puisque n est impair, 2 est inversible modulo n et on a

$$\begin{cases} a & \equiv a' \pmod n \\ b & \equiv b' \pmod n \end{cases}.$$

Comme $a, a' \in \mathbb{Z}_n,\ a \equiv a' \pmod n$ se simplifie en $a = a'$, et pareillement pour $b = b'$.
On a donc bien prouvé que $f_n(a, b) = f_n(a', b') \Rightarrow (a, b) = (a', b')$ et donc que f_n est injective. □

Corollaire 2.1.1. *Puisque* $|\text{dom } f_n| = |\text{im } f_n|,\ f_n$ *est bijective.*

On pourrait également prouver qu'elle est surjective.

Proposition 2.2. *La fonction* $f_n : (\mathbb{Z}_n)^2 \to (\mathbb{Z}_n)^2, (a, b) \mapsto (a+b \mod n, a-b \mod n)$ *est surjective.*

Démonstration. Soit $(c, d) \in (\mathbb{Z}_n)^2$.
Si c et d sont de même parité, $\frac{c+d}{2}$ est entier et $f_n(\frac{c+d}{2} \mod n, \frac{c-d}{2} \mod n) = (\frac{c+d}{2}+\frac{c-d}{2} \mod n, \frac{c+d}{2}-\frac{c-d}{2} \mod n) = (c, d)$.
Si ils sont de parités différentes, $\frac{c+n+d}{2}$ est entier et $f_n(\frac{c+n+d}{2} \mod n, \frac{c+n-d}{2} \mod n) = (\frac{c+n+d}{2} + \frac{c+n-d}{2} \mod n, \frac{c+n+d}{2} - \frac{c+n-d}{2} \mod n) = (c+n \mod n, d \mod n) = (c, d)$.
On a donc bien prouvé que $\forall (c, d) \in (\mathbb{Z}_n)^2,\ \exists (a, b) \in (\mathbb{Z}_n)^2 \mid f_n(a, b) = (c, d)$ et donc que f_n est surjective. □

2.3 Deuxième condition

Proposition 2.3. *Les fonctions* g_a, g_b, h_a, h_b *(définie dans la sous section 1.2) sont injectives.*

Démonstration. Prouvons que h_a est injective. Cette fonction est définie par $h_a : \mathbb{Z}_n \to \mathbb{Z}_n, b \mapsto a - b \mod n$.
Supposons que $h_a(b) = h_a(b')$, i.e. $a - b \mod n = a - b' \mod n \Leftrightarrow a - b \equiv a - b' \pmod n \Leftrightarrow b' \equiv b \pmod n$. Comme $b, b' \in \mathbb{Z}_n$, $b \equiv b' \pmod n$ se simplifie en $b = b'$.
On a donc bien prouvé que $h_a(b) = h_a(b') \Rightarrow b = b'$ et donc que h_a est injective.
La démonstration de l'injectivité de g_a, g_b, h_b est semblable. □

Corollaire 2.3.1. *Puisque* $|\text{dom } g_a| = |\text{im } g_a|, g_a$ *est bijective. Idem pour* g_b, h_a, h_b.

À nouveau, une preuve de la surjectivité.

Proposition 2.4. *Les fonctions* g_a, g_b, h_a, h_b *(définie dans la sous section 1.2) sont surjectives.*

Démonstration. Prouvons que h_b est surjective. Cette fonction est définie par $h_b : \mathbb{Z}_n \to \mathbb{Z}_n, a \mapsto a - b \mod n$.
Soit $d \in \mathbb{Z}_n$. $h_b(d + b \mod n) = h(d + b \mod n, b) = d + b - b \mod n = d$.
On a donc bien prouvé que $\forall d \in \mathbb{Z}_n, \exists a \in \mathbb{Z}_n \mid h_b(a) = d$ et donc que h_b est surjective.
La démonstration de la surjectivité de g_a, g_b, h_a est semblable. □

3 Composée

Il est également possible, à partir d'une solution du problème à $m \times m$ élèves et d'une à $n \times n$, d'en trouver une à $mn \times mn$ élèves.

La méthode utilisée pour composer deux fonctions ressemble à la division euclidienne. En effet, si l'on a les fonctions f_m et f_n qui sont solutions du problème, la solution du problème $mn \times mn$ obtenue par composée est définie par

$$f_m \boxtimes f_n(a,b) = f'_{mn}(a,b) = m \cdot f_n(\left\lfloor \frac{a}{m} \right\rfloor, \left\lfloor \frac{b}{m} \right\rfloor) + f_m(a \mod m, b \mod m). \tag{6}$$

Prouvons que cette fonction respecte les critères.

3.1 Exemple

Nous allons ici montrer à quoi ressemble un tableau généré par la fonction $f'_{15} = f_5 \boxtimes f_3$. Comme nous l'avons vu dans la définition, nous avons besoin des tableaux générés par les fonctions f_5 et f_3.

(0, 0)	(1, 4)	(2, 3)	(3, 2)	(4, 1)
(1, 1)	(2, 0)	(3, 4)	(4, 3)	(0, 2)
(2, 2)	(3, 1)	(4, 0)	(0, 4)	(1, 3)
(3, 3)	(4, 2)	(0, 1)	(1, 0)	(2, 4)
(4, 4)	(0, 3)	(1, 2)	(2, 1)	(3, 0)

(0, 0)	(1, 2)	(2, 1)
(1, 1)	(2, 0)	(0, 2)
(2, 2)	(0, 1)	(1, 0)

TABLE 4 – Les représentations des fonctions f_5 et f_3.

Essayons de calculer $f'_{15}(5,9)$. On a $5 = 1 \cdot 5 + 0$ et $9 = 1 \cdot 5 + 4$.
Donc, $f'_{15} = 5 \cdot f_3(1,1) + f_5(0,4) = 5 \cdot (2,0) + (4,1) = (14,1)$.

À titre d'exemple, on peut calculer quelques autres valeurs :
$f'_{15}(6,6) = 5 \cdot f_3(1,1) + f_5(1,1) = 5 \cdot (2,0) + (2,0) = (12,0)$
$f'_{15}(10,14) = 5 \cdot f_3(2,2) + f_5(0,4) = 5 \cdot (1,0) + (4,1) = (9,1)$
$f'_{15}(11,11) = 5 \cdot f_3(2,2) + f_5(1,1) = 5 \cdot (1,0) + (2,0) = (7,0)$.

(0, 0)	(1, 4)	(2, 3)	(3, 2)	(4, 1)	(5, 10)	(6, 14)	(7, 13)	(8, 12)	(9, 11)	(10, 5)
(1, 1)	(2, 0)	(3, 4)	(4, 3)	(0, 2)	(6, 11)	(7, 10)	(8, 14)	(9, 13)	(5, 12)	(11, 6)
(2, 2)	(3, 1)	(4, 0)	(0, 4)	(1, 3)	(7, 12)	(8, 11)	(9, 10)	(5, 14)	(6, 13)	(12, 7)
(3, 3)	(4, 2)	(0, 1)	(1, 0)	(2, 4)	(8, 13)	(9, 12)	(5, 11)	(6, 10)	(7, 14)	(13, 8)
(4, 4)	(0, 3)	(1, 2)	(2, 1)	(3, 0)	(9, 14)	(5, 13)	(6, 12)	(7, 11)	(8, 10)	(14, 9)
(5, 5)	(6, 9)	(7, 8)	(8, 7)	(9, 6)	(10, 0)	(11, 4)	(12, 3)	(13, 2)	(14, 1)	(0, 10)
(6, 6)	(7, 5)	(8, 9)	(9, 8)	(5, 7)	(11, 1)	(12, 0)	(13, 4)	(14, 3)	(10, 2)	(1, 11)
(7, 7)	(8, 6)	(9, 5)	(5, 9)	(6, 8)	(12, 2)	(13, 1)	(14, 0)	(10, 4)	(11, 3)	(2, 12)
(8, 8)	(9, 7)	(5, 6)	(6, 5)	(7, 9)	(13, 3)	(14, 2)	(10, 1)	(11, 0)	(12, 4)	(3, 13)
(9, 9)	(5, 8)	(6, 7)	(7, 6)	(8, 5)	(14, 4)	(10, 3)	(11, 2)	(12, 1)	(13, 0)	(4, 14)
(10, 10)	(11, 14)	(12, 13)	(13, 12)	(14, 11)	(0, 5)	(1, 9)	(2, 8)	(3, 7)	(4, 6)	(5, 0)
(11, 11)	(12, 10)	(13, 14)	(14, 13)	(10, 12)	(1, 6)	(2, 5)	(3, 9)	(4, 8)	(0, 7)	(6, 1)
(12, 12)	(13, 11)	(14, 10)	(10, 14)	(11, 13)	(2, 7)	(3, 6)	(4, 5)	(0, 9)	(1, 8)	(7, 2)
(13, 13)	(14, 12)	(10, 11)	(11, 10)	(12, 14)	(3, 8)	(4, 7)	(0, 6)	(1, 5)	(2, 9)	(8, 3)
(14, 14)	(10, 13)	(11, 12)	(12, 11)	(13, 10)	(4, 9)	(0, 8)	(1, 7)	(2, 6)	(3, 5)	(9, 4)

TABLE 5 – Une partie du tableau 15×15 généré par la fonction $f_5 \boxtimes f_3$.

Il est intéressant de remarquer que si deux couples ont le même reste après division euclidienne, il en est de même pour leurs images par f'_{15}. De même, si deux couples ont un même quotient après division euclidienne, leurs images aussi.

3.2 Première condition

Théorème 3.1. *Si f_m et f_n sont injectives, $f'_{mn} = f_m \boxtimes f_n$ l'est aussi.*

Démonstration. Supposons $f'_{mn}(a,b) = f'_{mn}(a',b')$. Si deux nombres sont égaux, les quotients et restes de leurs divisions euclidiennes par un nombre donné sont égaux. Or, $m \cdot f_n(\lfloor \frac{a}{m} \rfloor, \lfloor \frac{b}{m} \rfloor) + f_m(a \mod m, b \mod m)$ est le résultat de la division euclidienne de $f'_{mn}(a,b)$ par m, puisque $f_m(a \mod m, b \mod m)$ donne un couple dont les deux valeurs sont inférieures à m. De même, $m \cdot f_n(\lfloor \frac{a'}{m} \rfloor, \lfloor \frac{b'}{m} \rfloor) + f_m(a' \mod m, b' \mod m)$ est le résultat de la division euclidienne de $f'_{mn}(a',b')$ par m. Ainsi, comme deux nombres égaux ont des quotients et restes égaux après division par un nombre donné,

$$\begin{cases} f_n(\lfloor \frac{a}{m} \rfloor, \lfloor \frac{b}{m} \rfloor) & = f_n(\lfloor \frac{a'}{m} \rfloor, \lfloor \frac{b'}{m} \rfloor) \\ f_m(a \mod m, b \mod m) & = f_m(a' \mod m, b' \mod m) \end{cases}.$$

Comme les fonctions f_m et f_n sont injectives, cela implique directement

$$\begin{cases} (\lfloor \frac{a}{m} \rfloor, \lfloor \frac{b}{m} \rfloor) & = (\lfloor \frac{a'}{m} \rfloor, \lfloor \frac{b'}{m} \rfloor) \\ (a \mod m, b \mod m) & = (a' \mod m, b' \mod m) \end{cases}.$$

Finalement, on peut dire que deux nombres qui, lorsque divisés par un entier donné, ont les même quotients et restes sont forcement égaux, donc $(a,b) = (a',b')$.

On a donc bien prouvé que $f'_{mn}(a,b) = f'_{mn}(a',b') \Rightarrow (a,b) = (a',b')$ et donc que f'_{mn} est injective. □

Corollaire 3.1.1. *Puisque $|\text{dom } f'_{mn}| = |\text{im } f'_{mn}|$, f'_{mn} est bijective.*

Théorème 3.2. *Si f_m et f_n sont surjectives, $f'_{mn} = f_m \boxtimes f_n$ l'est aussi.*

Démonstration. Soit $(c,d) \in (\mathbb{Z}/mn\mathbb{Z})^2$. On définit le quotient et reste de (c,d) après division euclidienne par m :

$$(c,d) = m \cdot (c_q, d_q) + (c_r, d_r) \text{ où } c_r, d_r < m.$$

Puisque $c, d < mn, c_q, d_q < n$. Dés lors, comme f_m et f_n sont surjectives,

$$\exists (a_q, b_q) \in (\mathbb{Z}_n)^2, (a_r, b_r) \in (\mathbb{Z}_m)^2 \mid f_n(a_q, b_q) = (c_q, d_q), f_m(a_r, b_r) = (c_r, d_r).$$

En prenant $(a,b) = m \cdot (a_q, b_q) + (a_r, b_r)$ ((a_q, b_q) et (a_r, b_r) sont quotient et reste de (a,b)), on a

$$f'_m n(a,b) = m \cdot f_n(\lfloor \frac{a}{m} \rfloor, \lfloor \frac{b}{m} \rfloor) + f_m(a \mod m, b \mod m)$$

$$= m \cdot f_n(a_q, b_q) + f_m(a_r, b_r) = m \cdot (c_q, d_q) + (c_r, d_r) = (c,d).$$

On a donc bien prouvé que $\forall (c,d) \in (\mathbb{Z}/mn\mathbb{Z})^2,\ \exists (a,b) \in (\mathbb{Z}/mn\mathbb{Z})^2 \mid f'_{mn}(a,b) = (c,d)$ et donc que f'_{mn} est surjective. □

3.3 Deuxième condition

Théorème 3.3. *Si $g_{b,m}$ et $g_{n,a}$ sont injectives, $g'_{b,mn} = g_{b,m} \boxtimes g_{a,n}$ l'est aussi. Idem pour $g'_{a,mn}, h'_{a,mn}, h'_{b,mn}$.*

Démonstration. Supposons que $g'_{b,mn}(a) = g'_{b,mn}(a')$. Or, $g'_{b,mn}(a) = g'_{b,n}(\lfloor \frac{a}{m} \rfloor) + g_{b,m}(a \mod m)$ avec b_n fixé à $\lfloor \frac{b}{m} \rfloor$, et b_m fixé à $b \mod m$. On remarquera que $g'_{b,mn}(a) = g_{b,n}(\lfloor \frac{a}{m} \rfloor) + g_{b,m}(a \mod m)$ est le résultat de la division euclidienne de $g'_{b,mn}(a)$. Ainsi, par un raisonnement identique à celui du théorème 3.1, on a

$$\begin{cases} g_{b,n}(\lfloor \frac{a}{m} \rfloor) & = g_{b,n}(\lfloor \frac{a'}{m} \rfloor) \\ g_m(a \mod m) & = g'_m(a' \mod m) \end{cases} \Leftrightarrow \begin{cases} \lfloor \frac{a}{m} \rfloor & = \lfloor \frac{a'}{m} \rfloor \\ a \mod m & = a' \mod m \end{cases} \Leftrightarrow a = a'.$$

On a donc bien prouvé que $g'_{b,mn}(a) = g'_{b,mn}(a') \Rightarrow a = a'$ et donc que $g'_{b,mn}$ est injective.
La démonstration de l'injectivité de $g'_{a,mn}, h'_{a,mn}, h'_{b,mn}$ est semblable. □

Corollaire 3.3.1. *Puisque $|\text{dom } g'_{b,mn}| = |\text{im } g'_{b,mn}|$, $g'_{b,mn}$ est bijective. Idem pour $g'_{a,mn}, \ldots$.*

Théorème 3.4. *Si $g_{b,m}$ et $g_{b,n}$ sont surjectives, $g'_{b,mn} = g_{b,m} \boxtimes g_{b,n}$ l'est aussi. Idem pour $g'_{a,mn}, \ldots$.*

Démonstration. Soit $c \in \mathbb{Z}/mn\mathbb{Z}$. On effectue la division euclidienne :

$$c = m \cdot c_q + c_r \text{ où } c_r < m.$$

Puisque $c < mn, c_q < n$. Dés lors, comme $g_{b,m}$ et $g_{b,n}$ sont surjectives,

$$\exists a_q \in (\mathbb{Z}_n)^2, a_r \in (\mathbb{Z}_m)^2 \mid g_{b,n}(a_q) = c_q, g_{b,m}(a_r) = c_r).$$

En prenant $a = m \cdot a_q + a_r$ (a_q et a_r sont quotient et reste de a), on a

$$g_m n'(a) = m \cdot g_{b,n}(\lfloor \frac{a}{m} \rfloor) + g_{b,m}(a \mod m) = m \cdot g_{b,n}(a_q) + g_{b,m}(a_r) = m \cdot c_q + c_r = c.$$

On a donc bien prouvé que $\forall c \in \mathbb{Z}/mn\mathbb{Z},\ \exists a \in \mathbb{Z}/mn\mathbb{Z} \mid g'_{b,mn}(a) = c$ et donc que g_{mn} est surjective.
La démonstration de la surjectivité de $g'_{a,mn}, h'_{b,mn}, h'_{a,mn}$ est semblable. □

Lemme 3.5. *Si f_m et f_n sont des fonctions résolvant le problème, $f'_{mn} = f_m \boxtimes f_n$ l'est aussi.*

Démonstration. Si f_m et f_n sont des fonctions résolvant le problème, elles respectent toutes les deux la première condition, et par les corollaires des théorèmes 3.1 ou 3.2, la fonction f'_{mn} la respecte aussi.
De plus, f_m et f_n respectent également la deuxième condition, par hypothèse, et par les corollaires des théorèmes 3.3 et 3.4, la fonction f'_{mn} la respecte également.
Ainsi, $f'_{mn} = f_m \boxtimes f_n$ respecte les deux conditions et résout le problème. □

4 Généralisation

4.1 Puissances de 2

Maintenant que l'on peut faire des composées de fonctions (confer section 3), on peut s'attaquer aux nombres pairs, en commençant par les puissances de 2. À peu près par hasard, nous avons trouvé des solutions pour 2^2 et 2^3. Bien que pour le cas 2×2, il n'y ait pas de solution, pour toutes les autres puissances de 2, il en existe. Nous prouvons l'existence de ces solutions au point suivant. Cependant, pour se convaincre de la non existence d'une solution 2×2, on peut, par exemple, essayer toutes les configurations possibles, sachant qu'il n'y en a pas énormément. Néanmoins, ce raisonnement un peu brutal est beaucoup moins efficace pour montrer la non existence d'une solution 6×6 ou plus, car le nombre de cas à traiter explose rapidement.

4.1.1 Puissances paires

Lemme 4.1. *Il existe une solution de dimension* 4×4.

Démonstration. En voici une :

$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$
$(1,3)$	$(0,2)$	$(3,1)$	$(2,0)$
$(2,1)$	$(3,0)$	$(0,3)$	$(1,2)$
$(3,2)$	$(2,3)$	$(1,0)$	$(0,1)$

□

Théorème 4.2. *Pour tout naturel* n*, il existe une solution de dimension* $2^{2n} \times 2^{2n}$ *au problème.*

Démonstration. Par récurrence sur n.
Initialisation : Lorsque $n = 0$, il existe une solution évidente (le tableau de taille 1×1 contient un couple $(0,0)$).
Induction : Supposons que l'on ait une solution pour $2^{2n} \times 2^{2n}$. Alors, en la composant avec celle de 4×4, on obtient une solution pour $2^{2n} \cdot 4 \times 2^{2n} \cdot 4 = 2^{2n+2} \times 2^{2n+2}$. Cela clôt notre induction. □

4.1.2 Puissances impaires

Lemme 4.3. *Il existe une solution de dimension* 8×8.

Démonstration. En voici une :

$(0,0)$	$(1,1)$	$(2,2)$	$(3,3)$	$(4,4)$	$(5,5)$	$(6,6)$	$(7,7)$
$(5,6)$	$(4,7)$	$(7,4)$	$(6,5)$	$(1,2)$	$(0,3)$	$(3,0)$	$(2,1)$
$(2,3)$	$(3,2)$	$(0,1)$	$(1,0)$	$(6,7)$	$(7,6)$	$(4,5)$	$(5,4)$
$(7,5)$	$(6,4)$	$(5,7)$	$(4,6)$	$(3,1)$	$(2,0)$	$(1,3)$	$(0,2)$
$(4,1)$	$(5,0)$	$(6,3)$	$(7,2)$	$(0,5)$	$(1,4)$	$(2,7)$	$(3,6)$
$(1,7)$	$(0,6)$	$(3,5)$	$(2,4)$	$(5,3)$	$(4,2)$	$(7,1)$	$(6,0)$
$(6,2)$	$(7,3)$	$(4,0)$	$(5,1)$	$(2,6)$	$(3,7)$	$(0,4)$	$(1,5)$
$(3,4)$	$(2,5)$	$(1,6)$	$(0,7)$	$(7,0)$	$(6,1)$	$(5,2)$	$(4,3)$

□

Théorème 4.4. *Pour tout naturel* n*, il existe une solution de dimension* $2^{2n+3} \times 2^{2n+3}$.[3]

Démonstration. Par le théorème 4.2, il existe une solution pour 2^{2n}. En la composant avec celle de 8×8, on obtient une solution pour $2^{2n} \cdot 8 \times 2^{2n} \cdot 8 = 2^{2n+3} \times 2^{2n+3}$. □

Corollaire 4.4.1. *Pour tout naturel* $n \neq 1$*, il existe une solution de taille* $2^n \times 2^n$.

3. Remarquons que ainsi, le cas 2×2 est exclus, mais toutes les autres puissances impaires de 2 sont incluses.

4.2 Multiples de 4

Tous les multiples de 4 peuvent être écrits comme un produit d'un nombre impair et d'une puissance supérieure à 2 de 2. On a vu, dans la section 2 qu'il existait une solution pour tout nombre impair. Par le corollaire 4.4.1, on sait qu'il en existe pour toute puissance supérieure à 2 de 2. De plus, par le lemme 3.5, s'il existe des solutions pour $m \times m$ et $n \times n$, il en existe pour $mn \times mn$. Ainsi, il existe une solution pour tous les multiples de 4.

4.3 Et le reste ?

Les nombres pairs non multiples de 4 résistent encore et toujours.. On s'aperçoit facilement qu'il n'y a pas de solution de dimension 2×2, mais ça se complique dés le 6×6. C'est d'ailleurs ce que le très célèbre mathématicien Leonhard Euler conjectura en 1782 dans son problème des 36 officiers :

> You're in command of an army that consists of six regiments, each containing six officers of six different ranks. Can you arrange the officers in a 6×6 square so that each row and each column of the square holds only one officer from each regiment and only one officer from each rank ?

5 Annexe

5.1 Arithmétique modulaire

5.1.1 Théorème de Bézout

Soient a et b entiers. On peut écrire n comme combinaison linéaire de a et b ssi n est multiple de $\gcd(a, b)$.

5.1.2 Congruence

On dit que deux nombres a et b sont congrus modulo n ssi leur différence est multiple de n, i.e. ssi ils ont le même reste après division par n. On écrit $a \equiv b \pmod{n}$.
On a évidement certaines propriétés :
Si $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}, a \equiv c \pmod{n}$.
Si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, $\begin{cases} a + c & \equiv b + d \\ a - c & \equiv b - d \\ a \cdot c & \equiv b \cdot d \end{cases} \pmod{n}$.

5.1.3 Inverse

On défini l'inverse de a modulo n comme étant l'entier a^{-1} tel que $aa^{-1} \equiv 1 \pmod{n}$. Cela est équivalent à $aa^{-1} + kn = 1$ pour certains a^{-1}, k entiers. Par le théorème de Bézout, cela est possible ssi 1 est multiple de $\gcd(a, n)$, i.e. ssi $\gcd(a, n) = 1$. En d'autres termes, a possède un inverse modulo n ssi il est premier avec n.

5.1.4 Ensemble des entiers

Lorsqu'on travaille modulo n, $n \equiv 0,\ n + 1 \equiv 1,\ \ldots$. On peut alors considérer que ces nombres sont égaux, et que les seuls nombres existant sont $0, 1, \ldots, n - 1$. Dans ce cas, on travaille dans l'ensemble des entiers modulo n, $\{0, 1, 2, \ldots, n - 2, n - 1\}$, dénoté $\mathbb{Z}_n$.

5.2 Injection, surjection et bijection

En mathématiques, les injections, les surjections et les bijections sont des fonctions qui se distinguent par la manière dont les arguments (expressions d'entrée du domaine) et les images (expressions de sortie du codomaine) sont liés l'un à l'autre.

5.2.1 Injectivité

Une fonction est injective ssi toute image a au plus un antécédent, i.e. est l'image d'au plus un élément du domaine. Formellement, on a $f : X \to Y, x \mapsto f(x)$ est injective ssi

$$\forall x,\ x' \in X : x \neq x' \Rightarrow f(x) \neq f(x') \Leftrightarrow f(x) = f(x') \Rightarrow x = x'.$$

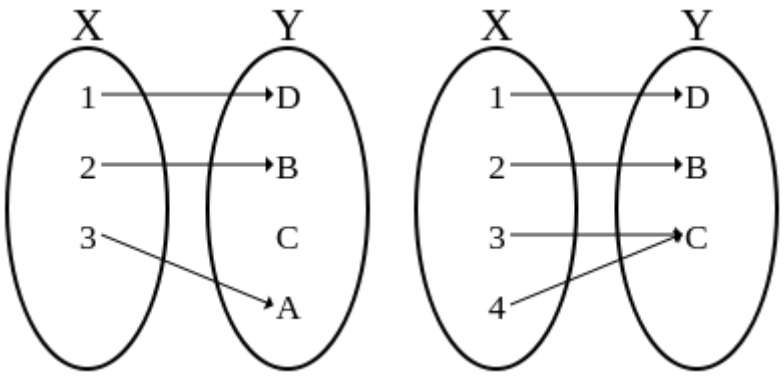

FIGURE 1 – *À gauche :* fonction injective. *À droite :* fonction non-injective.

On dit que f est une injection de X vers Y.

5.2.2 Surjectivité

Une fonction est surjective ssi toute image a au moins un antécédent, i.e. est l'image d'au moins un élément du domaine. Formellement, $f : X \to Y, x \mapsto f(x)$ est surjective ssi

$$\forall y \in Y, \exists x \mid f(x) = y.$$

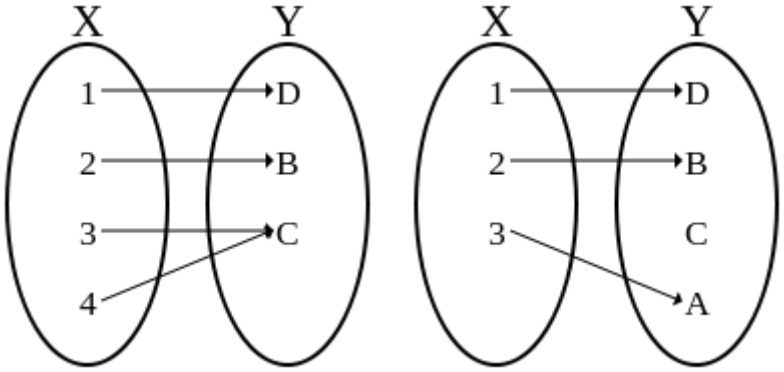

FIGURE 2 – *À gauche :* fonction surjective. *À droite :* fonction non-surjective.

On dit que f est une surjection de X vers Y.

5.2.3 Bijectivité

Une fonction est bijective ssi toute image a exactement un antécédent, i.e. est l'image d'exactement un élément du domaine. Par les définition d'injectivité et de surjectivité, on remarque qu'une fonction est bijective ssi elle est injective et surjective. De manière formelle, $f : X \to Y, x \mapsto f(x)$ est bijective ssi

$$\forall x,\ x' \in X : f(x) = f(x') \Rightarrow x = x' \text{ et } \forall y \in Y, \exists x \mid f(x) = y.$$

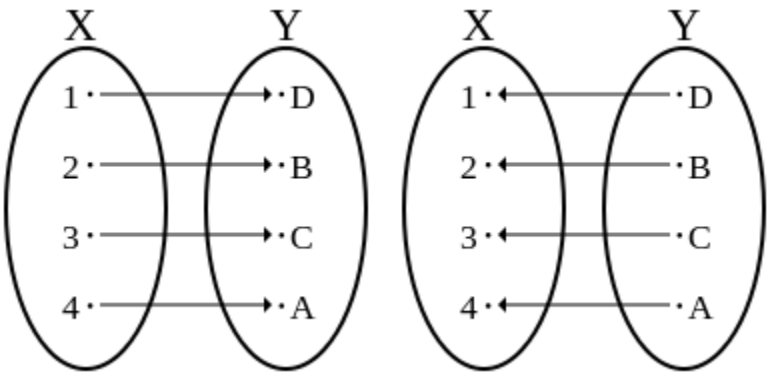

FIGURE 3 – Fonction bijective et son inverse.

On dit que f est une bijection de X vers Y. Lorsque f est bijective, on peut définir $f^{-1} : Y \to X, f(x) \mapsto x$, qui est aussi bijective.