# Chapitre 5

# Systèmes de restes chinois

## 5.1 Un exemple de problème

Trois pilotes d'avion aimeraient à l'occasion dîner ensemble à Paris. Ils se concertent un dimanche par SMS et constatent que :

1. André se rendra à Paris le mardi suivant et y retournera tous les 5 jours.
2. Bernard se rendra à Paris le mercredi suivant et y retournera tous les 8 jours.
3. Cloé se rendra à Paris le jeudi suivant et y retournera tous les 13 jours.

Quand est-ce qu'ils pourront se retrouver pour dîner ?

## 5.2 Le ppcm

### Définition

Soit $a$ et $b$ deux nombres entiers.

On définit le *plus petit commun multiple de $a$ et $b$*, noté $\text{ppcm}(a, b)$, comme étant le plus petit nombre positif qui est multiple à la fois de $a$ et de $b$.

### Exemples

1. On a $\text{ppcm}(12, 14) = 84$.

   En effet, l'ensemble des multiples positifs (ou nul) de 12 est
   $$M_{12} = \{0, 12, 24, 36, 48, 60, 72, 84, 96, \ldots\}$$
   et l'ensemble des multiples positifs (ou nul) de 14 est
   $$M_{14} = \{0, 14, 28, 42, 56, 70, 84, 98, \ldots\}$$
   L'ensemble des multiples positifs (ou nul) commun à 12 et à 14 est donc $M_{12} \cap M_{14} = \{0, 84, 168, 252, \ldots\}$. Ainsi, le plus petit commun multiple est 84.

2. On a aussi $\text{ppcm}(2, 3) = 6$.

3. Ou encore $\text{ppcm}(7, -21) = 21$.

### Le cas particulier du zéro

Lorsqu'un des deux termes est nul (ou les deux), on est obligé d'admettre la valeur 0 pour le ppcm. Autrement dit, on a $\text{ppcm}(0, b) = 0$ pour tout $b \in \mathbb{Z}$.

**Résultat**

Soit $a$ et $b$ deux entiers. Alors $\text{ppcm}(a,b) \cdot \text{pgcd}(a,b) = |ab|$.

**Preuve**

On va montrer que $\frac{|ab|}{\text{pgcd}(a,b)} = \text{ppcm}(a,b)$. On a :

$$\frac{|ab|}{\text{pgcd}(a,b)} = \frac{\pm|a|}{\text{pgcd}(a,b)} \cdot b = \frac{\pm|b|}{\text{pgcd}(a,b)} \cdot a \quad \text{où} \quad \frac{\pm|a|}{\text{pgcd}(a,b)} \text{ et } \frac{\pm|b|}{\text{pgcd}(a,b)} \in \mathbb{Z}$$

on constate ainsi que $\frac{|ab|}{\text{pgcd}(a,b)}$ est un multiple de $a$ et de $b$. C'est le plus petit possible, puisqu'on ne peut pas diviser $a$ et $b$ par un nombre plus grand que $\text{pgcd}(a,b)$. □

## 5.3 Résolution de systèmes de restes chinois

**Le théorème des restes chinois**

Soit $a_1$ et $a_2$ deux nombres entiers. Soit $m_1$ et $m_2$ deux nombres naturels.

Le système suivant possède une solution si et seulement si $a_1 \equiv a_2 \pmod{\text{pgcd}(m_1,m_2)}$.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

De plus, si une solution existe, elle est unique modulo $\text{ppcm}(m_1,m_2)$.

**Preuve**

Il existe $k_1$ et $k_2 \in \mathbb{Z}$ tels qu'on a les équivalences :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \iff \begin{cases} x = a_1 + k_1 m_1 \\ x = a_2 + k_2 m_2 \end{cases}$$

$$\overset{\text{subst.}}{\iff} \begin{cases} x = a_1 + k_1 m_1 \\ a_1 + k_1 m_1 = a_2 + k_2 m_2 \end{cases} \iff \begin{cases} x = a_1 + k_1 m_1 \\ k_1 m_1 - k_2 m_2 = a_2 - a_1 \end{cases}$$

Ainsi le système de restes chinois admet une solution si et seulement si l'équation diophantienne $k_1 m_1 - k_2 m_2 = a_2 - a_1$ (d'inconnues $k_1$ et $k_2$) admet une solution. Or dans le résultat d'existence, on a vu que c'est le cas si et seulement si $\text{pgcd}(m_1,m_2)$ divise $a_2 - a_1$. Autrement dit $a_1 \equiv a_2 \pmod{\text{pgcd}(m_1,m_2)}$.

Pour l'unicité, prenons deux solutions $x_1$ et $x_2$ du système de restes chinois et montrons qu'elles sont égales modulo $\text{ppcm}(m_1,m_2)$.

Puisque $x_1 \equiv a_1$ et $x_2 \equiv a_1$ modulo $m_1$, on a $x_1 \equiv x_2 \pmod{m_1}$. De même, on a $x_1 \equiv x_2 \pmod{m_2}$. Ainsi, on a $x_1 - x_2 = k_1 m_1$ avec $k_1 \in \mathbb{Z}$ et $x_1 - x_2 = k_2 m_2$ avec $k_2 \in \mathbb{Z}$. On obtient ainsi une équation diophantienne $k_1 m_1 - k_2 m_2 = 0$. Les solutions de cette équation homogène sont

$$k_1 = \frac{m_2}{\text{pgcd}(m_1,m_2)} k \quad \text{et} \quad k_2 = \frac{m_1}{\text{pgcd}(m_1,m_2)} k \quad \text{avec} \quad k \in \mathbb{Z}$$

Donc

$$x_1 - x_2 = \frac{m_1 m_2}{\text{pgcd}(m_1,m_2)} k = \text{ppcm}(m_1,m_2) k$$

C'est-à-dire que $x_1 \equiv x_2 \pmod{\text{ppcm}(m_1,m_2)}$. □

**Pour la résolution**

Lorsqu'on veut résoudre un système chinois à deux équations, on suit le principe de la démonstration en utilisant l'équivalence établie dans la preuve ci-dessus.

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \iff \begin{cases} x = a_1 + k_1 m_1 \\ k_1 m_1 - k_2 m_2 = a_2 - a_1 \quad \textit{«équation diophantienne»} \end{cases}$$

Il faut ainsi chercher $k_1$ (et $k_2$) en résolvant l'équation diophantienne à l'aide de l'algorithme d'Euclide étendu. On aura ainsi l'équivalence suivante (démontrée dans la preuve ci-dessus) où $k_1$ est la solution trouvée :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases} \iff x \equiv a_1 + k_1 m_1 \pmod{\text{ppcm}(m_1, m_2)}$$