5.13 1) Soient $(\overline{r}_i\,;\overline{s}_j) \in (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$.

Puisque m et n sont premiers entre eux, le théorème chinois des restes garantit que le système de congruences

$$\begin{cases} x \equiv r_i \mod m \\ x \equiv s_j \mod n \end{cases}$$

possède une unique solution modulo mn. On définit $\overline{a}_{ij}$ comme étant l'unique élément de $\mathbb{Z}/mn\mathbb{Z}$ solution de ce système de congruences.

Après avoir vérifié que cette application est bien définie, prouvons qu'elle est injective.

Supposons que $(\overline{r}_i\,;\overline{s}_j) \longmapsto \overline{a}_{ij}$, que $(\overline{r}_k\,;\overline{s}_l) \longmapsto \overline{b}_{kl}$ et que $\overline{a}_{ij} = \overline{b}_{kl}$.
Il s'agit de montrer que $(\overline{r}_i\,;\overline{s}_j) = (\overline{r}_k\,;\overline{s}_l)$.

Les exercices 5.3 et 5.4 assurent les équivalences suivantes :

$$\overline{a}_{ij} = \overline{b}_{kl} \quad\Longleftrightarrow\quad a_{ij} \equiv b_{kl} \mod mn \quad\Longleftrightarrow\quad \begin{cases} a_{ij} \equiv b_{kl} \mod m \\ a_{ij} \equiv b_{kl} \mod n \end{cases}$$

Il en résulte par conséquent :

$$\begin{cases} r_i \equiv a_{ij} \equiv b_{kl} \equiv r_k \mod m \\ s_j \equiv a_{ij} \equiv b_{kl} \equiv s_l \mod n \end{cases} \quad \text{c'est-à-dire} \quad \begin{cases} \overline{r}_i = \overline{r}_k \\ \overline{s}_j = \overline{s}_l \end{cases}$$

2) (a) $a_{ij} \equiv r_i \mod m$ équivaut à $a_{ij} = r_i + m\,q$ pour un certain $q \in \mathbb{Z}$.
L'exercice 3.2 donne $\mathrm{D}(a_{ij}, m) = \mathrm{D}(a_{ij} - m\,q, m) = \mathrm{D}(r_i, m)$.
Il en résulte que $\mathrm{pgcd}(a_{ij}, m) = \mathrm{pgcd}(r_i, m)$.

Comme $\overline{r}_i$ est un élément inversible de $\mathbb{Z}/m\mathbb{Z}$, r_i et m sont premiers entre eux : $\mathrm{pgcd}(r_i, m) = 1$.
Il s'ensuit que a_{ij} et m sont aussi premiers entre eux.

(b) $a_{ij} \equiv s_j \mod n$ équivaut à $a_{ij} = s_j + n\,q^\star$ pour un certain $q^\star \in \mathbb{Z}$.
L'exercice 3.2 donne $\mathrm{D}(a_{ij}, n) = \mathrm{D}(a_{ij} - n\,q^\star, n) = \mathrm{D}(s_j, n)$.
Il en résulte que $\mathrm{pgcd}(a_{ij}, n) = \mathrm{pgcd}(s_j, n)$.

Comme $\overline{s}_j$ est un élément inversible de $\mathbb{Z}/n\mathbb{Z}$, s_j et n sont premiers entre eux : $\mathrm{pgcd}(s_j, n) = 1$.
Il s'ensuit que a_{ij} et n sont aussi premiers entre eux.

(c) D'après le théorème de Bézout, il existe des entiers u, v, x, y tels que

$$a_{ij}\,u + m\,v = 1 \quad \text{et} \quad a_{ij}\,x + n\,y = 1\,.$$

En multipliant ces deux équations, on obtient :

$$a_{ij}\,(a_{ij}\,u\,x + n\,u\,y + m\,v\,x) + m\,n\,v\,y = 1\,.$$

Le théorème de Bachet de Mériziac implique $\mathrm{pgcd}(a_{ij}, mn) = 1$.

3) (a) D'après le théorème chinois des restes, il existe un unique a modulo mn tel que $\begin{cases} a \equiv r \mod m \\ a \equiv s \mod n \end{cases}$.
Si l'on avait $\overline{r} = \overline{r}_i$ pour un certain $1 \leqslant i \leqslant \varphi(m)$ et $\overline{s} = \overline{s}_j$ pour un certain $1 \leqslant j \leqslant \varphi(n)$, alors $\overline{a}$ serait forcément égal à $\overline{a}_{ij}$.

Puisque l'on suppose le contraire, $\overline{r} \neq \overline{r}_i$ pour tout $1 \leqslant i \leqslant \varphi(m)$ ou $\overline{s} \neq \overline{s}_j$ pour tout $1 \leqslant j \leqslant \varphi(n)$. En d'autres termes, $r \notin (\mathbb{Z}/m\mathbb{Z})^*$ ou $s \notin (\mathbb{Z}/n\mathbb{Z})^*$.

(b) $a \equiv r \mod m$ équivaut à $a = r + m\,q$ pour un certain $q \in \mathbb{Z}$.

L'exercice 3.2 donne $\mathrm{D}(a, m) = \mathrm{D}(a - m\,q, m) = \mathrm{D}(r, m)$.

Il en résulte que $\mathrm{pgcd}(a, m) = \mathrm{pgcd}(r, m) > 1$.

Puisque tout diviseur de m divise a fortiori mn, on conclut que $\mathrm{pgcd}(a, mn) \geqslant \mathrm{pgcd}(a, m) > 1$.

Ainsi, a et mn ne sont pas premiers entre eux, si bien que $\overline{a}$ n'est pas un élément inversible de $\mathbb{Z}/mn\mathbb{Z}$.

(c) $a \equiv s \mod n$ équivaut à $a = s + n\,q^\star$ pour un certain $q^\star \in \mathbb{Z}$.

L'exercice 3.2 donne $\mathrm{D}(a, n) = \mathrm{D}(a - n\,q^\star, n) = \mathrm{D}(s, n)$.

Il en résulte que $\mathrm{pgcd}(a, n) = \mathrm{pgcd}(s, n) > 1$.

Puisque tout diviseur de n divise a fortiori mn, on conclut que $\mathrm{pgcd}(a, mn) \geqslant \mathrm{pgcd}(a, n) > 1$.

Ainsi, a et mn ne sont pas premiers entre eux, si bien que $\overline{a}$ n'est pas un élément inversible de $\mathbb{Z}/mn\mathbb{Z}$.

4) Nous avons montré en 2) que l'application définie en 1) est injective.

En 3), nous avons établi que l'application définie en 1) a pour image l'ensemble des éléments inversibles de $\mathbb{Z}/mn\mathbb{Z}$.

Par conséquent, il y a une bijection entre l'ensemble des unités de $\mathbb{Z}/mn\mathbb{Z}$ et $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$. D'où la formule $\varphi(mn) = \varphi(m)\,\varphi(n)$.