Théorème de l'isomorphisme chinois.

i) Soient $m, n \geqslant 1$ des entiers premiers entre eux. Alors l'application

$$\mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$x \bmod mn \longmapsto (x \bmod m, x \bmod n)$$

est un isomorphisme d'anneaux.

ii) En particulier cela induit un isomorphisme des groupes des inversibles

$$(\mathbb{Z}/mn\mathbb{Z})^* \simeq (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^* \ .$$

iii) D'où l'égalité des cardinaux

$$|(\mathbb{Z}/mn\mathbb{Z})^*| = \varphi(mn) = \varphi(m)\varphi(n) = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| \ .$$

Démo. En effet, soient n^* et m^* les inverses respectifs de n dans $\mathbb{Z}/m\mathbb{Z}$ et de m dans $\mathbb{Z}/n\mathbb{Z}$. † Voici la réciproque du morphisme d'anneaux de l'énoncé :

$$(a \bmod m, b \bmod n) \mapsto an^*n + bm^*m \bmod mn \ ‡ \ .$$

†. *c-à-d* $nn^* = 1 \bmod m$ et $mm^* = 1 \bmod n$.

‡. On a bien $\forall\, a, b \in \mathbb{Z}$, $an^*n + bm^*m = a \bmod m$ et $b \bmod n$. En particulier $n^*n + m^*m = 1 \bmod mn$ vu que $m \wedge n = 1$.