Exercice 1 Soient a et b des entiers supérieurs ou égaux à 2 et soient d leur pgcd et m leur ppcm. Notons $a = da'$, $b = db'$ et $d = au + bv$. Soit $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ définie par

$$f(x, y) \ := \ (ux + vy, -b'x + a'y) \ .$$

Soient $p : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ et $q : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ les applications données par le produit des surjections canoniques.

1. Montrer que f est un morphisme de groupes.
2. Montrer que f est un isomorphisme (on calculera son inverse g).
3. Montrer qu'il existe un unique morphisme de groupes
$$f' : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$
tel que $p \circ f = f' \circ q$ (respectivement $q \circ g = g' \circ p$).
4. Montrer que f' et g' sont inverses l'un de l'autre.

Exercice 2 Soient a et b des entiers supérieurs ou égaux à 2. On note d (resp. m) leur pgcd (resp. ppcm). On notera $a = da'$ et $b = db'$ et l'on fixera de plus un couple d'entiers (u, v) tel que $au + bv = d$.

1. Montrer que les formules :
$$\begin{aligned} x \mod m &\mapsto (x \mod a, x \mod b) \\ (x \mod a, y \mod b) &\mapsto (y - x) \mod d \end{aligned}$$
définissent bien respectivement des applications
$$\begin{aligned} \iota \ : \ \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \pi \ : \ \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\to \mathbb{Z}/d\mathbb{Z} \ . \end{aligned}$$
2. Les applications π et ι sont-elles des morphismes de groupes ? d'anneaux ?
3. Montrer que $\mathrm{Im}\iota \subset \mathrm{Ker}\pi$.
4. Montrer que π est surjective.
5. Montrer que ι est injectif.
6. Montrer finalement que $\mathrm{Im}\iota = \mathrm{Ker}\pi$.
7. Comment interpréter le résultat précédent en termes de résolution de système de congruence ?

Exercice 3 Soit $n \geq 1$ un entier. On notera $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la projection canonique.

1. Soit $f : (\mathbb{Z}n\mathbb{Z}, +) \to (\mathbb{Z}/n\mathbb{Z}, +)$ un morphisme de groupes.
   (a) Montrer que pour tout entiers $x, y \in \mathbb{Z}$ on a $f[\pi(x) \cdot \pi(y)] = \pi(x)f[\pi(y)]$.
   (b) En déduire que
   $$\forall (\alpha, \beta) \in (\mathbb{Z}/n\mathbb{Z})^2, \ \text{ on a } \ f(\alpha \cdot \beta) \ = \ \alpha f(\beta) \ .$$

2. Soit f un automorphisme du groupe additif $\mathbb{Z}/n\mathbb{Z}$.
   (a) Montrer que $f(1)$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$.
   (b) En déduire que η définie par $\eta(f) := f(1)$ est une application de l'ensemble $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ dans l'ensemble $(\mathbb{Z}/n\mathbb{Z})^{\times}$.
   (c) Montrer que l'application η st un morphisme de groupes.
3. À tout $\alpha \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ on associe $\theta(\alpha)$ l'application de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même définie par
$$\forall \beta \in \mathbb{Z}/n\mathbb{Z}, \quad \theta(\alpha)(\beta) = \alpha\beta \ .$$
   (a) Montrer que $\forall \alpha (\mathbb{Z}/n\mathbb{Z})^{\times}$ on a $\theta(\alpha) \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$.
   (b) Montrer que l'application θ ainsi définie est un morphisme.
   (c) Si η désigne l'application définie précédemment, montrer que θ et η sont inverses l'un de l'autre.
4. Déduire des questions précédentes que, pour tout $n \in \mathbb{N}^*$ le groupe symétrique $\mathcal{S}_n$ possède un sous-groupe abélien de cardinal $\phi(n+1)$ où ϕ désigne l'indicatrice d'Euler.