Réduction des inversibles modulo n

Il est utile de se remémorer la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ dans le *Cours d'Algèbre* de D. Perrin.

Exercice. Soient $k, n \geqslant 1$ deux entiers tels que $k \mid n$. On considère le morphisme d'anneaux $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ de réduction modulo k. Le but de cet exercice est d'étudier l'image et le noyau du morphisme de groupes $f_{n,k} : (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/k\mathbb{Z})^\times$ induit sur les éléments inversibles.

(1) Montrez que $f_{n,k}$ est surjectif.

(2) Soit Σ_n l'ensemble des nombres premiers qui divisent n, appelé *support de n*. Montrez qu'il existe un unique couple (n_1, n_2) d'entiers naturels tels que $n = n_1 n_2$, $\Sigma_{n_1} = \Sigma_k$ et $\Sigma_{n_2} \cap \Sigma_k = \varnothing$. Montrez que $k \mid n_1$ et qu'on a un isomorphisme $\ker(f_{n,k}) \simeq \ker(f_{n_1,k}) \times (\mathbb{Z}/n_2\mathbb{Z})^\times$.

L'étude de $f_{n_1,k}$ nous ramène donc au cas où $\Sigma_n = \Sigma_k$, ce que l'on suppose dans toute la suite.

(3) Soient $a, b \geqslant 1$ deux entiers. Montrez que $\Sigma_a = \Sigma_b$ si et seulement si $\varphi(a)/a = \varphi(b)/b$, où φ est l'indicatrice d'Euler. Déduisez-en le cardinal de $\ker(f_{n,k})$.

(4) En décomposant n en facteurs premiers, montrez que l'on a :

(i) si $8 \nmid n$ ou $4 \mid k$: $\ker(f_{n,k}) \simeq \mathbb{Z}/l\mathbb{Z}$ où $n = kl$. Donnez un générateur explicite.

(ii) si $8 \mid n$ et $4 \nmid k$: $\ker(f_{n,k}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2l\mathbb{Z}$ où $n = 4kl$. Donnez deux générateurs explicites.

On peut donc dire que lorsque $\Sigma_n = \Sigma_k$, le morphisme $f_{n,k}$ s'insère dans à une suite exacte :

(i) si $8 \nmid n$ ou $4 \mid k$: $0 \longrightarrow \mathbb{Z}/l\mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{f_{n,k}} (\mathbb{Z}/k\mathbb{Z})^\times \longrightarrow 1$,

(ii) si $8 \mid n$ et $4 \nmid k$: $0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2l\mathbb{Z} \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{f_{n,k}} (\mathbb{Z}/k\mathbb{Z})^\times \longrightarrow 1$.