Arithmétique

Exercice 1. — Soit $n \geqslant 1$ un entier.

a) Pour $k \in \mathbf{Z}$, montrer que $\overline{k} \in \mathbf{Z}/n\mathbf{Z}$ est inversible ssi $k \wedge n = 1$.
En pratique, comment détermine-t-on l'inverse d'un élément non nul ?
A.N. : Quel est l'inverse de 47 modulo 97 ?

b) Quels sont les sous-groupes de $(\mathbf{Z}/n\mathbf{Z}, +)$?

c) Pour $k \in \mathbf{Z}$, quel est le sous-groupe de $(\mathbf{Z}/n\mathbf{Z}, +)$ engendré par $\overline{k}$? Quel est son ordre ?

d) Donner tous les générateurs des groupes $(\mathbf{Z}/5)^\times$, $(\mathbf{Z}/7)^\times$ et $(\mathbf{Z}/11)^\times$.

Exercice 2. — Soient m et n deux entiers positifs.

a) Si m et n sont premiers entre eux, rappeler l'énoncé du lemme chinois.
Dans ce cas, expliciter l'isomorphisme inverse.

b) Lorsque m et n ne sont plus premiers entre eux, existe-t-il un isomorphisme (éventuellement donné par une autre formule) entre ces anneaux ?

c) Résoudre dans $\mathbf{Z}$:

$$\begin{cases} x \equiv 1\ [7] \\ x \equiv 3\ [5] \end{cases}, \quad \begin{cases} x \equiv 1\ [45] \\ x \equiv 3\ [6] \end{cases}, \quad \begin{cases} x \equiv 4\ [45] \\ x \equiv 1\ [6] \end{cases}$$

Exercice 3. — **a)** Rappeler comment calculer $\varphi(n)$ à partir d'une factorisation en facteurs premiers de n. Calculer $\varphi(7)$, $\varphi(8)$ et $\varphi(21)$.

b) Pour $k \geqslant 1$ fixé, montrer que l'ensemble $\{n \in \mathbf{N}, \varphi(n) = k\}$ est fini.
[**Indication:** Commencer par montrer que les facteurs premiers possibles pour un tel n sont finis.]
Déterminer cet ensemble pour $k = 2^5$, $k = 2 \cdot 7^3$.

c) En déduire que $\lim\limits_{n\to\infty} \varphi(n) = +\infty$.

Exercice 4. — **[Nombres de Carmichael]**
Soit $n \geqslant 2$ un entier.

a) En utilisant le critère de Fermat, comment peut-on montrer que n n'est pas premier, sans exhiber de factorisation de n ?

Un entier $n \geqslant 2$ est dit *de Carmichael* si n n'est pas premier mais vérifie tout de même :

$$\forall\, a \in \mathbf{Z},\ a^n \equiv a[n].$$

b) Montrer qu'un entier $n = p_1 \dots p_k$ (les p_i étant premiers et distincts) tel que pour tout i, $p_i - 1 | n - 1$ est de Carmichael.
Vérifier que $561 = 3 \cdot 11 \cdot 17$ est de Carmichael.

c) Montrer que tout entier de Carmichael est de la forme précédente avec $k \geqslant 3$.
[**Indication:** Commencer par montrer que n est sans facteur carré. Puis, utiliser que pour p premier, $(\mathbf{Z}/p)^\times$ contient un élément d'odre $p - 1$. Enfin, montrer que $k = 2$ est impossible.]

On sait depuis 1994 qu'il existe une infinité de nombres de Carmichael.

d) Si n n'est pas de Carmichael, montrer que l'ensemble

$$\{a \in (\mathbf{Z}/n\mathbf{Z})^\times,\ a^{n-1} \not\equiv 1\} > \{a \in (\mathbf{Z}/n\mathbf{Z})^\times,\ a^{n-1} \equiv 1\}.$$

Ainsi, en tirant au hasard a, on a plus d'une chance sur 2 qu'il montre que n est composé.