TD n° 4

Exercice 1.

On considère le groupe ($Z/11Z \setminus \{\bar{0}\}$, $\times$).

1) Déterminer l'ordre de $\bar{1}$ dans ($Z/11Z \setminus \{\bar{0}\}$, $\times$).

2) Déterminer l'ordre de $\bar{2}$ dans ($Z/11Z \setminus \{\bar{0}\}$, $\times$).

3) Montrer que ($Z/11Z \setminus \{\bar{0}\}$, $\times$) est un groupe cyclique.

Exercice 2.

1) Déterminer l'ordre de $\bar{4}$ dans le groupe $(\mathbf{Z}/24\mathbf{Z},+)$.

2) On note $(\Omega_{63},\times)$ désigne le groupe des racines $63^{\text{ème}}$ de l'unité .

Vérifier $w = e^{\frac{10i\pi}{21}}$ est un élément de Ω_{63} puis détérminer son ordre dans le groupe $(\Omega_{63},\times)$

Exercice 3.

On note U_{15} l'ensemble des inversibles de l'anneau $Z/15Z$.

Considérons le morphisme de groupes $f : U_{15} \to U_{15}$ défini par : $f(\bar{x}) = \bar{x}^2$

1) Résoudre dans Z , l'équation $x^2 \equiv 1\ [15]$

2) Déterminez $\ker(f)$ puis calculez l'ordre de chaque élément de $\ker(f)$

3) En déduire $(U_{15},\times)$ n'est pas cyclique

Exercice 4.

1) Résoudre dans $\mathbf{Z}$, les systèmes suivants :

(1) $\begin{cases} 2x \equiv 7\ [13] \\ x \equiv -1\ [11] \end{cases}$; (2) $\begin{cases} 5x \equiv -4\ [8] \\ 2x \equiv 6\ [7] \end{cases}$; (3) $\begin{cases} 5x \equiv 4\ [6] \\ 16x \equiv 13\ [7] \end{cases}$; (4) $\begin{cases} 2x \equiv 7\ [5] \\ x \equiv 10\ [11] \end{cases}$

Exercice 5.

Dans un chiffrement utilisant le code RSA modulo n et de clé public e, Alice publie $(n = 26,\ e = 7)$ et reçoit de Bob le message m^7

Comment pourra-t-elle le déchiffrer ?

Exercice 6

Soit $n = pq = 8871979$ un produit de deux nombres premiers.

Sachant que $\varphi(n) = 8866000$ où φ désigne la fonction indicatrice d'Euler, retrouver alors la factorisation de l'entier n