Examen final

Tous les résultats devront être soigneusement justifiés.
Les calculatrices, ainsi que tous documents ***ne sont pas autorisés****.*
Les téléphones portables doivent être rangés et éteints.

Exercice 1 On pose

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 6 & 3 & 7 & 8 & 2 & 11 & 1 & 12 & 4 & 10 & 9 \end{pmatrix} \in S_{12}.$$

1. Déterminer σ^{-1}.
2. Décomposer σ en produit de cycles à supports disjoints.
3. Quel est l'ordre de σ ?
4. Calculer σ^{2019}.

Exercice 2

1. Déterminer l'ensemble des solutions dans $\mathbb{Z}^2$ de l'équation $48x + 66y = 8$.
2. Déterminer l'ensemble des solutions dans $\mathbb{Z}^2$ de l'équation $48x + 66y = 6$.

Exercice 3

1. Calculer le reste de la division euclidienne de 3^{2019} par 21 et par 80.
2. Résoudre le système de congruences

$$\begin{cases} x \equiv 6 \mod 21 \\ x \equiv 27 \mod 80 \end{cases}.$$

3. En déduire le reste de la division euclidienne de 3^{2019} par 1680.

Exercice 4

On pose $G = \mathbb{Z}/20\mathbb{Z}$. On note $\overline{k}$ la classe de $k \in \mathbb{Z}$ dans G. On note $G^\times$ le groupe pour la loi $\times$ constitué des éléments de G qui sont inversibles pour la multiplication.

1. Quel est l'ordre de $\overline{16}$ dans le goupe $(G, +)$.
2. L'élément $\overline{16}$ appartient-il à $G^\times$?
3. Montrer que $\overline{17} \in G^\times$ et déterminer son inverse.
4. Déterminer le cardinal de $G^\times$.
5. Montrer que G est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et donner un isomorphisme explicite.
6. Montrer que $G^\times$ est isomorphe au groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.
7. Le groupe $G^\times$ est-il cyclique ? Justifiez votre réponse.

Exercice 5 Montrer que l'application $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{R},\ (a,b) \mapsto a + b\sqrt{5}$ est un morphisme de groupes dont on donnera l'image et le noyau. Justifier que $H = \{a + b\sqrt{5} \mid a,\ b \in \mathbb{Z}\}$ est un sous-groupe de $\mathbb{R}$.

Exercice 6

Soient p et q deux nombres premiers distincts. On pose $n = pq$.

1. Soit $d \in \mathbb{Z}$ premier avec $(p-1)(q-1)$. Justifier qu'il existe $e \in \mathbb{Z}$ tel que
$$de \equiv 1 \mod (p-1)(q-1).$$
2. Montrer que pour tout $t \in \mathbb{Z}$,
$$t^{de} \equiv t \mod p.$$
3. Montrer que pour tout $t \in \mathbb{Z}$,
$$t^{de} \equiv t \mod n.$$