Exercice 1 (*Extrait du sujet 2007*)

Soit G un groupe multiplicatif de cardinal fini $N \in \mathbb{N}^*$.

1. Montrer que a^{N-1} est un inverse de a dans G.
2. On considère la décomposition en base 2 de $N-1$:

$$N-1 = \sum_{i=0}^{k} x_i 2^i \quad \text{avec } k \in \mathbb{N},\ x_i \in \{0,1\},\ i \in \{0,1,\dots,k\} \text{ et } x_k \neq 0.$$

On considère les suites finies $(a_i)_{0\leq i\leq k+1}$ et $(b_i)_{0\leq i\leq k+1}$ définies par :

$$a_0 = 1, \quad b_0 = a, \quad \forall i \in \{0,1,\dots,k\}, \quad a_{i+1} = a_i b_i^{x_i}, \quad b_{i+1} = b_i^2.$$

(a) Montrer que a_{k+1} est l'inverse de a dans G.

(b) En déduire un algorithme de calcul de a^{-1} et préciser en fonction de k son coût (*i.e.* le nombre maximum de multiplications dans G que nécessite le calcul de a^{-1}). L'algorithme doit prendre comme argument a et N.

Exercice 2 (*Extrait du sujet 2007*)

Soit G le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$.

1. Déterminer le cardinal N de G.
2. Démontrer que 5 est un élément de G et déterminer son inverse par la méthode de la question 2(b) de l'exercice 1.
3. Donner une autre méthode pour déterminer cet inverse.

Exercice 3 (*Extrait du sujet 2008*)

1. Soit $M \in GL_n(\mathbb{Z})$ d'ordre $m \geq 2$. Soit p un nombre premier tel que $p \geq 3$. On suppose que $M = I_n + p^r N$ avec $r \in \mathbb{N}^*$ et $N \in \mathcal{M}_n(\mathbb{Z}) \setminus p\mathcal{M}_n(\mathbb{Z})$ (où $p\mathcal{M}_n(\mathbb{Z})$ est l'ensemble des matrices de $\mathcal{M}_n(\mathbb{Z})$ dont tous les coefficients sont des multiples de p).
   (a) Montrer que $mp^r N \in p^{2r}\mathcal{M}_n(\mathbb{Z})$. En déduire que p divise m.
   (b) On pose $m = pm'$ et $M' = M^p$. Montrer que p divise m'.
   (c) Conclure une contradiction.
2. Soit p un nombre premier tel que $p \geq 3$. Soit G un sous-groupe fini de $GL_n(\mathbb{Z})$. On rappelle que la surjection naturelle $\mathbb{Z} \longrightarrow \mathbb{F}_p$ induit un morphisme de groupes $GL_n(\mathbb{Z}) \longrightarrow GL_n(\mathbb{F}_p)$. Montrer que G est isomorphe un sous-groupe de $GL_n(\mathbb{F}_p)$.
3. Soit G un sous-groupe fini de $GL_2(\mathbb{Z})$. Montrer que le cardinal G est un diviseur de 48.

Exercice 4 (*Extrait du sujet 2009*)

1. Soit $\mathbb{K}$ un corps de caractéristique différente de 2. Soit $n \geq 1$. Soit G un sous-groupe multiplicatif de $GL_n(\mathbb{K})$ tel que pour tout $M \in G$, $M^2 = I_n$.
   Montrer que G est abélien de cardinal inférieur ou égal 2^n.
2. En déduire que pour tout $(m,n) \in (\mathbb{N}^*)^2$, les groupes multiplicatifs $GL_n(\mathbb{K})$ et $GL_m(\mathbb{K})$ sont isomorphes si et seulement si $n = m$.