UNIVERSITÉ PARIS DIDEROT - PARIS 7
Année 2007-2008, Licence 2, MI4, Groupes et arithmétique

Examen partiel du 01/03/08 (durée : 2 heures)
Les documents et la calculatrice ne sont pas autorisés

I

1. Utiliser l'algorithme d'Euclide pour calculer le PGCD des entiers 92 et 68 (écrire toutes les étapes).
2. Pour chacune des équations suivantes, dire si elle a ou non des solutions dans $\mathbb{Z}^2$:
   (a) $92x + 68y = 10$,
   (b) $92x + 68y = 12$.

II

Décomposer en produit de cycles disjoints la permutation σ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$$

Déterminer l'ordre et la signature de σ. Calculer σ^{2008}.

III

1. Donner l'ordre de chacun des éléments du groupe $\mathbb{Z}/8\mathbb{Z}$.
2. Montrer que pour tout $k \in \mathbb{Z}$, l'application $f_k : \mathbb{Z}/8\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ définie par $f_k(\overline{a}) = \overline{ka}$ est un morphisme de groupe.
3. Montrer que le morphisme f_k défini précédemment est bijectif si et seulement si $\overline{k}$ est un élément d'ordre 8 dans $\mathbb{Z}/8\mathbb{Z}$ (i. e. un générateur de $\mathbb{Z}/8\mathbb{Z}$).
   On note A l'ensemble des morphismes f_k qui sont bijectifs.
4. Montrer que A contient quatre éléments et décrire chacun d'eux.
5. Compléter la table de composition des éléments de A. Quel est l'ordre de chacun des éléments de A dans le groupe des bijections de $\mathbb{Z}/8\mathbb{Z}$?

IV

On rappelle que pour $n \geq 1$, et $0 \leq k \leq n$, les coefficients binomiaux C_n^k sont les coefficients du polynôme $(1 + X)^n$; ce sont des entiers donnés par la formule :

$$\mathrm{C}_n^k = \frac{n \times (n-1) \times \cdots \times (n-k+1)}{k!} .$$

Soit p un nombre premier.

1. Montrer que pour $0 < k \leq p$, p divise $k! \times C_p^k$.
2. Montrer que pour $0 < k < p$, p est premier avec $k!$.
3. Montrer que pour $0 < k < p$, p divise C_p^k.
4. Montrer par récurrence que pour tout entier $k \in \mathbb{N}$, $k^p - k$ est divisible par p.
5. En déduire une preuve (autre que celle du cours) du théorème de Fermat : Pour tout entier k premier avec p, le nombre k^{p-1} est congru à 1 modulo p.