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

Examen partiel du 03/12/07 (durée : 2 heures)

I

1. Utiliser l'algorithme d'Euclide pour calculer le PGCD des entiers 4732 et 4572 (écrire toutes les étapes).
2. Quelles sont les solutions dans $\mathbb{Z}^2$ de l'équation :

$$4732x + 4572y = 7 \ ?$$

II

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. Démontrer que pour $0 < k < p$, p divise C_p^k.
4. Démontrer par récurrence que pour tout entier $k \in \mathbb{N}$, $k^p - k$ est divisible par p.
5. En déduire une nouvelle preuve du théorème de Fermat : Pour tout entier k premier avec p, le nombre k^{p-1} est congru à 1 modulo p.

III

Soit p un nombre premier, et $M_p = 2^p - 1$ (M_p est appelé un nombre de Mersenne).

1. Soit q un nombre premier qui divise M_p.
   (a) Calculer $\overline{2}^p$ dans $\mathbb{Z}/qZ$.
   Quel est l'ordre de $\overline{2}$ dans le groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z} - \{\overline{0}\}$?
   (b) Calculer $\overline{2}^{q-1}$ dans $\mathbb{Z}/qZ$. En déduire que p divise $q-1$.
2. Utiliser ce qui précède pour déterminer si $M_{11} = 2047$ est premier.

IV

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}.