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. $92 = 68 + 24$,
   $68 = 2 \times 24 + 20$,
   $24 = 20 + 4$,
   $20 = 5 \times 4$.
   Le PGCD est 4.
2. (a) $92x + 68y = 10$ n'a pas de solution : 10 n'est pas multiple du PGCD de 92 et 68.
   (b) $92x + 68y = 12$ a des solutions : $12 = 3 \times 4$; le PGCD de 92 et 68 divise 12.

II

$$\sigma = (12345)(67)\ ,\ \sigma \text{ est d'ordre } 10\ .$$
$$\sigma^{2008} = \sigma^{10} = (12345)^{10}(67)^{10}\ ,$$
$$\sigma^{2008} = (12345)^3 = (14253)\ ,$$
$$\sigma^{2008} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 5 & 1 & 2 & 3 & 6 & 7 & 8 \end{pmatrix}\ .$$

III

1.

élément	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
ordre	1	8	4	8	2	8	4	8

2. L'application f_k est bien définie : si $\overline{a} = \overline{a'}$, alors $a' - a$ est un multiple de 8 ; $ka' - ka$ est aussi un multiple de 8 et donc $\overline{ka} = \overline{ka'}$.
   Pour toutes les classes $\overline{a}$ et $\overline{b}$ dans $\mathbb{Z}/8\mathbb{Z}$, on a :

$$\begin{aligned} f_k(\overline{a} + \overline{b}) &= f_k(\overline{a+b}) \\ &= \overline{k(a+b)} \\ &= \overline{ka + kb} \\ &= \overline{ka} + \overline{kb} \\ &= f_k(\overline{a}) + f_k(\overline{b}) \end{aligned}$$

3. $\mathbb{Z}/8\mathbb{Z}$ étant fini, pour que l'application f_k soit bijective il faut et il suffit qu'elle soit surjective. L'image de f_k est le sous-groupe engendré par $f(k) = \overline{k}$. Donc f est un isomorphisme si et seulement si $\overline{k}$ est d'ordre 8.

4. f_k ne dépend que de la valeur de $\overline{k}$ modulo 8. D'après la question précédente et la question 1,
$$A = \{f_1, f_3, f_5, f_7\} .$$

x	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$f_1(x)$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$f_3(x)$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$f_5(x)$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$f_7(x)$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

5.

	f_1	f_3	f_5	f_7
f_1	f_1	f_3	f_5	f_7
f_3	f_3	f_1	f_7	f_5
f_5	f_5	f_7	f_1	f_3
f_7	f_7	f_5	f_7	f_1

f_1 est d'ordre 1 ; f_3,f_5,f_7 sont d'ordre 2.

IV

1. Pour $0 < k \leq p$, on a : $k!C_p^k = p(p-1)\dots(p-k+1)$.
   Comme $k \geq 1$, le produit de droite comporte au moins le facteur p : p divise $k! \times C_p^k$.
2. p étant premier est premier avec 2, 3, …,$p-1$. D'après le lemme d'Euclide, pour $0 < k < p$, p est premier avec le produit : $2 \times 3 \times \cdots \times k = k!$.
3. On applique le théorème de Gauss : p divise $k! \times C_p^k$, et p est premier avec $k!$, donc p divise C_p^k.
4. Pour $k = 0$, $k^p - k = 0$ est divisible par p.
   Supposons que pour $k \geq 0$, $k^p - k$ est divisible par p, alors :
$$(1+k)^p = 1 + C_p^1 k + \cdots + C_p^{p-1}k^{p-1} + k^p \equiv 1 + k^p \pmod{p} .$$
   Par hypothèse de récurrence : $(1+k)^p \equiv 1 + k \pmod{p}$, i.e. p divise $(1+k)^p - (1+k)$.
5. On vient de montrer que p divise $k(k^{p-1}-1)$. Pour k est premier avec p, le lemme de Gauss montre que p divise $k^{p-1}-1$. Donc $k^{p-1} \equiv 1 \pmod{p}$.