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

Examen du 13/05/08 (durée : 2 heures)

Document autorisé : résumé de cours manuscrit sur une page recto-verso de format A4 (21×29,7). La calculatrice est autorisée.

I

L'armée de César comptait plus de 1000 hommes, mais moins de 3000. Lorsqu'il voulut la dénombrer par groupes de 11, il n'en resta pas ; par groupes de 9, il en resta 5 ; par groupes de 13, il en resta 8. Combien y avait-il de soldats dans cette armée ?

II

1. Décrire succintement une méthode pour montrer qu'un nombre est premier. Application : montrer que 787 est premier (on ne demande pas les détails de calcul).
2. Calculer le symbole de Legendre $\left(\frac{238}{787}\right)$.
3. Est-ce que 238 est un carré modulo 787 ?

III

1. Soit $p = 8k + 7$ un nombre premier.
   (a) Que vaut le symbole de Legendre $\left(\frac{2}{p}\right)$?
   (b) Montrer que $2^{4k+3} - 1$ est divisible par p.
2. (a) Vérifier que 263 est premier.
   (b) Est-ce que le nombre de Mersenne $M_{131} = 2^{131} - 1$ est premier ?

IV

1. Soit $N > 2$, et b un entier tel que :
   a) $b^{N-1} \equiv 1 \bmod N$,
   b) $b^d \not\equiv 1 \bmod N$ pour tout diviseur d de $N - 1$ autre que $N - 1$.
   Que peut-on dire de l'ordre de $\overline{b}$ dans le groupe des éléments inversibles de $\mathbb{Z}/N\mathbb{Z}$?
   Montrer que N est premier.
2. Montrer que si on remplace la condition b) par :
   c) $b^d \not\equiv 1 \bmod N$ pour tout diviseur d de $N - 1$ de la forme $d = \frac{N-1}{q}$, avec q diviseur premier de $N - 1$,
   on obtient la même conclusion.
3. Décomposer 8460 en facteurs premiers.
4. Appliquer la question 2 à $N = 8461$ et $b = 23$.
5. Quel est le nombre de générateurs du groupe des inversibles de $\mathbb{Z}/8461\mathbb{Z}$?