

UNIVERSITÉ PARIS DIDEROT - PARIS 7
Année 2008-2009, Licence 2, MI4
Groupes et arithmétique

Examen du 02/06/08 (durée : 3 heures)

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

La calculatrice est autorisée.

On demande de rédiger les détails de calcul.

I

Calculer le pgcd d de 17640 et 525. Déterminer deux entiers u et v tels que l'on ait

$$d = 17640u + 525v .$$

II

Résoudre les systèmes de congruence :

a)

$$\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 5 \pmod{15} \end{cases}$$

b)

$$\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 5 \pmod{15} \\ x \equiv 7 \pmod{17} \end{cases}$$

III

1. Vérifier que 983 est premier (donner brièvement l'argument).
2. Calculer le symbole de Legendre $\left(\frac{610}{983}\right)$.
3. Est-ce que 610 est un carré modulo 983 ?
4. Sans nouveau calcul, montrer que 610^{491} est congru à 1 modulo 983.
5. Montrer que pour x entier, x^2 est congru à 610 modulo 983 si et seulement si x est congru à $\pm 610^{246}$ modulo 983.
6. Utiliser la décomposition de 246 en somme de puissances de 2 pour calculer 610^{246} modulo 983.

IV

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

1. Soit q un nombre premier qui divise M_p .
 - (a) Montrer que : $2^p \equiv 1$ modulo q .
 - (b) Quel est l'ordre de $\bar{2}$ dans le groupe multiplicatif $\mathcal{U}(\mathbb{Z}/q\mathbb{Z})$?
 - (c) Dédire que p divise $q - 1$.
2. Utiliser ce qui précède pour déterminer si $M_{11} = 2047$ est premier.