UNIVERSITÉ PARIS DIDEROT - PARIS 7
Année 2012-2013, Licence 2, MI4
Groupes et arithmétique

Examen du 17/05/2013 (durée : 2 heures)

Document autorisé : une copie du résumé de cours mis en ligne (annotations personnelles en marge acceptées). La calculatrice est autorisée (pas de téléphone).

I

1. Démontrer que 13 et 280 sont premiers entre eux et trouver un couple de Bezout.
2. On considère la clé publique RSA $(319, 13)$, c'est à dire que le module est $n = pq = 319$, et l'exposant est $c = 13$.
   (a) Quel est le cryptage avec cette clé de $m = 10$?
   (b) Factoriser 319 et calculer la clé privée d.
   (c) Déchiffrer le message $m' = 133$.

II

1. Décomposer 1729 en facteurs premiers.
2. Rappeler ce qu'est un nombre de Carmichael.
3. Est-ce que 1729 est un nombre de Carmichael ? Justifier avec précision.

   Pour $k \in \mathbb{N}^*$, on pose :

$$N_k = a_k b_k c_k \ , \text{ avec } a_k = 6k+1 \ , \ b_k = 12k+1 \ , \ c_k = 18k+1 \ .$$

4. Calculer N_1. Est-ce un nombre de Carmichael ?
5. Est-ce que N_2 est un nombre de Carmichael ?
6. Montrer que $N_k - 1$ est divisible par $36k$.
7. Montrer que si les trois nombres a_k, b_k et c_k sont premiers, alors N_k est un nombre de Carmichel.
8. Est-ce que N_6 est un nombre de Carmichael.

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. Expliquer comment calculer 610^{246} modulo 983 avec l'algorithme des puissances rapides.