Université Paris Est Créteil Val de Marne
Licences d'Informatique et de Mathématiques
2009-2010

Mathématiques discrètes pour l'informatique
Examen du 20 mai 2010. Durée 2 heures.
(Sans documents. Les calculatrices sont autorisées.)

Question 1 : PGCD et PPCM

1. Soient deux entiers naturels non nuls a et b. Montrez que a et b sont premiers entre eux si et seulement si $PPCM(a, b) = ab$.
2. Déterminez l'ensemble des couples (a, b) d'entiers naturels non nuls vérifiant

$$2PPCM(a, b) + 3PGCD(a, b) = 159.$$

Question 2 : Congruences

1. Déterminez l'inverse de 17 dans $\mathbb{Z}/64\mathbb{Z}$.
2. Résolvez le système suivant :

$$\begin{cases} 2x \equiv 7(mod\ 9) \\ 7x \equiv 9(mod\ 11) \end{cases}$$

Question 3 : RSA
On considère le système cryptographique RSA avec la clé publique $(n, e) = (159, 57)$.

1. Est-ce que le couple (n, e) est une clé publique possible pour RSA ? Justifiez.
2. Quelle est la clé secrète $(\varphi(n), d)$ qui permet de décoder les messages ?
3. Quel est le cryptogramme du message $M = 125$?
4. On déchiffre $C = 70$. Quelle est la valeur du message ?

Question 4 : Séries génératrices
On considère la suite (a_n) :

$$\begin{cases} a_0 = 1 \\ a_1 = 5 \\ a_n = 5a_{n-1} - 6a_{n-2} \quad \forall n \geq 2 \end{cases}$$

1. Déterminez la forme close de la série génératrice correspondante.
2. Déterminez le terme général a_n.