

Mathématiques discrètes pour l'informatique

Session 2, le 30 juin 2010. Durée 2 heures.

(Sans documents. Les calculatrices sont autorisées.)

Question 1 : Graphes

Dessinez le graphe G ayant la matrice d'adjacence suivante :

$$M = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Déterminez les degrés intérieur et extérieur de chaque sommet. Donnez un circuit dans le graphe G . Le graphe G est-il fortement connexe ?

Question 2 : Congruences

1. Déterminez l'inverse de 7 dans $\mathbb{Z}/64\mathbb{Z}$.
2. Résolvez le système suivant :

$$\begin{cases} x \equiv 7 \pmod{9} \\ x \equiv 9 \pmod{11} \end{cases}$$

Question 3 : RSA

On considère le système cryptographique RSA avec la clé publique $(n, e) = (77, 53)$.

1. Le couple (n, e) est-il 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 $M = 25$?
4. On déchiffre $C = 60$. Quelle est la valeur du message ?

Question 4 : Séries génératrices

On considère la suite (a_n) :

$$\begin{cases} a_0 = 1 \\ a_1 = 5 \\ a_n = 5a_{n-1} - 4a_{n-2} \quad \forall n \geq 2 \end{cases}$$

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