

Mathématiques discrètes pour l'informatique

Session 2, le 29 juin 2011. Durée 2 heures.

(Sans documents. Les calculatrices sont autorisées.)

Le barème est donné à titre indicatif.

Question 1. (5 points)

Propriété 1. Dans un groupe de n personnes, il y a toujours au moins deux personnes ayant le même nombre d'amis présents.

1. Formulez cette propriété sous forme de graphe, en précisez bien ce que représente vos sommets et vos arêtes.
2. Démontrez la propriété.

Question 2 : Congruences (3 points)

1. Résolvez l'équation suivante :

$$7x \equiv 10 \pmod{35}.$$

2. Résolvez le système suivant :

$$\begin{cases} 17x \equiv 66 \pmod{67} \\ 17x \equiv 22 \pmod{23} \end{cases}$$

Question 3 : L'algorithme à clé publique RSA (6 points)

1. Montrez que le couple $(91, 23)$ est une clé publique possible pour RSA ?
2. Quelles sont les clés secrètes correspondantes $(\varphi(n), d)$?
3. Quels sont les cryptogrammes du message $M = 125$?
4. On déchiffre $C = 8$. Quels sont les messages correspondantes ?

Question 4 : Séries génératrices (6 points)

On considère la suite (a_n) :

$$\begin{cases} a_0 = \frac{17}{21} \\ a_1 = 2 \\ a_n = \frac{17}{2}a_{n-1} - \frac{21}{2}a_{n-2} \quad \forall n \geq 2 \end{cases}$$

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