

**Mathématiques discrètes pour l'informatique**

Session 2, le 20 juin 2012. Durée 2 heures.

*(Sans documents. Les calculatrices sont autorisées.)*

Le barème est donné à titre indicatif.

**Question 1. Graphe (3 points)**

Dessiner tous les arbres (deux à deux non isomorphes) qui ont 7 sommets.

**Question 2 : Congruences (3 points)**

1. Résoudre la congruence suivante :

$$23x \equiv 12 \pmod{76}$$

2. Résoudre le système suivant :

$$\begin{cases} 23x \equiv 12 \pmod{76} \\ 17x \equiv 13 \pmod{37} \end{cases}$$

**Question 3 : L'algorithme à clé publique RSA (8 points)**

1. Parmi les couples  $(97, 68)$ ,  $(1139, 115)$ , et  $(2813, 119)$ , lesquels sont des clés publiques possibles pour RSA ? Justifier.
2. Quelles sont les clés secrètes correspondantes  $(\varphi(n), d)$  ?
3. Quels sont les cryptogrammes du message  $M = 212$  ?
4. On déchiffre  $C = 151$ . Quels sont les messages correspondantes ?

**Question 4 : Séries génératrices (6 points)**

Trouver le terme général de la suite  $(a_n)$  définie ci-dessous

$$\begin{cases} a_0 = 11 \\ a_1 = 52 \\ a_n = 7a_{n-1} - 10a_{n-2} \quad \forall n \geq 2 \end{cases}$$