

**Mathématiques discrètes pour l'informatique**

Session 2, le 19 juin 2013. Durée 2 heures.

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

Le barème est donné à titre indicatif.

**Question 1. PGCD et PPCM (4 points)**

Déterminer l'ensemble des couples  $(a, b)$  d'entiers naturels vérifiant

$$a + PGCD(a, b) + PPCM(a, b) = 9.$$

**Question 2 : Congruences (4 points)**

Résoudre le système suivant :

$$\begin{cases} 27x \equiv 20 \pmod{29} \\ 17x \equiv 13 \pmod{54} \end{cases}$$

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

On considère le système cryptographique RSA avec la clé publique  $(n, e) = (4819, 157)$ .

1. Quel est le cryptogramme du message  $M = 199$ ?
2. On déchiffre  $C = 196$ . Quel est le message correspondant ?

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

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

$$\begin{cases} a_0 = 5 \\ a_1 = 19 \\ a_n = 8a_{n-1} - 15a_{n-2} \quad \forall n \geq 2 \end{cases}$$