

**Mathématiques discrètes pour l'informatique**

Examen du 22 mai 2013. Durée 2 heures.

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

Le barème est donné à titre indicatif.

**Question 1. Indicatrice d'Euler (4 points)**

Pour tout entier  $n \geq 2$ , on note  $\varphi(n)$  son indicatrice d'Euler, c'est-à-dire le nombre d'entiers compris entre 1 et  $n$  qui sont premiers avec  $n$ . Soient  $p, q$  deux nombres premiers distincts et  $\alpha, \beta$  deux nombre naturels non nuls.

1. Exprimer  $\varphi(p^\alpha)$  en fonction de  $p$  et  $\alpha$ .
2. Exprimer  $\varphi(p^\alpha q^\beta)$  en fonction de  $p, q, \alpha, \beta$ .

**Question 2 : Congruences (4 points)** Résoudre le système suivant :

$$\begin{cases} 29x \equiv 12 \pmod{47} \\ 37x \equiv 23 \pmod{53} \end{cases}$$

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

1. Montrer que le couple  $(n, e) = (3977, 157)$  est une clé publique possible pour RSA.
2. Quelle est la valeur de  $\varphi(n)$ ? Quelle est la clé secrète correspondante  $d$ ?
3. Quel est le cryptogramme du message  $M = 124$ ?
4. On déchiffre  $C = 171$ . Quel est le message correspondant?

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

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

$$\begin{cases} a_0 = 21 \\ a_1 = 203 \\ a_n = 13a_{n-1} - 30a_{n-2} \quad \forall n \geq 2 \end{cases}$$