

Mathématiques discrètes pour l'informatique

Examen du 19 mai 2011. Durée 2 heures.

(Sans documents. Les calculatrices sont autorisées.)

Le barème est donné à titre indicatif.

Question 1. (3 points)

1. Soit n un nombre naturel plus grand ou égal à 2. On considère p le plus petit nombre naturel tel que p divise n et $p \geq 2$. Montrez que p est un nombre premier.
2. Montrez que l'ensemble des nombres premiers est infini.
3. Déterminez l'ensemble des couples (a, b) de nombres naturels non nuls vérifiant

$$\text{pgcd}(a, b) + \text{ppcm}(a, b) = a + b + 6.$$

Question 2 : Congruences (3 points)

1. Déterminez l'inverse de 30 dans $\mathbb{Z}/67\mathbb{Z}$.
2. Résolvez le système suivant :

$$\begin{cases} 30x \equiv 7 \pmod{67} \\ 11x \equiv 9 \pmod{23} \end{cases}$$

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

1. Parmi les couples $(897, 70)$, $(899, 77)$ et $(3599, 77)$, lesquels sont des clés publiques possibles pour RSA ? Justifiez.
2. Quelles sont les clés secrètes correspondantes $(\varphi(n), d)$?
3. Quels sont les cryptogrammes du message $M = 125$?
4. On déchiffre $C = 1$. Quels sont les messages correspondants ?

Question 4 : Séries génératrices (6 points)

On considère la suite (a_n) :

$$\begin{cases} a_0 = 1 \\ a_1 = 7 \\ a_n = 7a_{n-1} - 12a_{n-2} \quad \forall n \geq 2 \end{cases}$$

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