

Mathématiques discrètes pour l'informatique

Examen du 18 mai 2012. Durée 2 heures.

(Sans documents. Les calculatrices sont autorisées.)

Le barème est donné à titre indicatif.

Question 1. Nombres de Mersenne (3 points)

Soient $a \geq 2$ et $n \geq 2$ deux entiers. Si $a^n - 1$ est un nombre premier, montrer que $a = 2$ et n est un premier.

Les nombres de Mersenne sont les nombres de la forme $M_p = 2^p - 1$, avec p premier. Pour montrer qu'un nombre de Mersenne n'est pas nécessairement premier, justifier que M_{11} n'est pas premier.

Question 2 : Congruences (3 points)

1. Résoudre la congruence suivante :

$$27x \equiv 12 \pmod{31}$$

2. Résoudre le système suivant :

$$\begin{cases} 27x \equiv 12 \pmod{31} \\ 17x \equiv 13 \pmod{52} \end{cases}$$

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

1. Parmi les couples $(89, 21)$, $(120, 68)$ et $(1513, 101)$, 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 $M = 100$?
4. On déchiffre $C = 169$. Quels sont les messages correspondantes ?

Question 4 : Séries génératrices (6 points)

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

$$\begin{cases} a_0 = 3 \\ a_1 = 8 \\ a_n = 6a_{n-1} - 8a_{n-2} \quad \forall n \geq 2 \end{cases}$$