Université du Littoral Côte d'Opale | Année universitaire 2013–2014
Licence 2ème année | Informatique

Calcul Formel & Courbes et Surfaces

Durée : 2 h le jeudi 3 juillet
Documents et calculatrices personnelles autorisés

Exercice 1. On pose $p = 3$ et $q = 7$ et $e = 5$

1. Calculer $n = p \cdot q$ puis $\varphi(n)$.

2. Déterminer les éléments inversibles de $\mathbb{Z}/12\mathbb{Z}$ et donner leurs inverses.

3. Chercher d tel qu'on ait $ed \equiv 1 \mod \varphi(n)$.

4. Quels paramètres constituent la clé publique ? Et la clé privée ?

5. Posons $M = 3$. Quel est le chiffré C de M ?

6. Retrouver M à partir de C et de la clé privée.

Exercice 2. *Supposons que nous ayons une classe (ou structure)* `Matrice` *permettant de représenter les matrices carrées à coefficients dans* $\mathbb{Z}$ *(les entiers sont représentés par le type* `int`*). Les fonctions utiles sont:*

- `Matrice M(n)` qui crée une matrice de taille `n` $\times$ `n`;
- `M[i][j]` qui accède au coefficient à la position (`i`, `j`) de la matrice `M`, les indices commençant à 1;
- `M.taille` qui retourne la taille de `M`.

Une matrice carrée $A = (a_{i,j})$ *de taille* $n \times n$ *est dite symétrique si* $a_{i,j}$ *est égale à* $a_{j,i}$ *pour tous les couples* (i, j) *de* $\{1, ..., n\}^2$.

1. Parmi les matrices suivantes, lesquelles sont symétriques :

$$A_1 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix},\ A_2 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix},\ A_3 = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix},\ A_4 = \begin{bmatrix} 2 & -1 & 1 \\ -1 & 1 & 2 \\ 1 & 2 & -1 \end{bmatrix}$$

2. Ecrire en pseudo-langage ou en `C++` une fonction `est_symétrique(Matrice A)` qui retourne `true` si `A` est symétrique et `false` sinon.

Soit $A = (a_{i,j})$ *une matrice carrée, la matrice transposée de* A*, notée* ${}^tA$ *est la matrice* ${}^tA = (a_{j,i})$. *Exemple :*

$$A_5 = \begin{bmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \\ 1 & 3 & 2 \end{bmatrix} \quad et \quad {}^tA_5 = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

3. Calculer la transposée des matrices A_1, A_2, A_3 et A_4.

4. Ecrire en pseudo-langage ou en `C++` une fonction `transposee(Matrice A)` qui retourne la transposée de la matrice `A`.

On dit qu'une matrice carrée A *est un carré magique si les sommes des coefficients sur chaque ligne et chaque colonne sont égales.*

5. Trouver les trois carrés magiques parmi A_1, A_2, A_3, A_4 et A_5.

6. Ecrire en pseudo-langage ou en `C++` les fonctions `int somme_ligne(Matrice A,int i)` et `int somme_colonne(Matrice A,int j)` qui retourne respectivement la somme des coefficients de la ligne `i` de `A` et la somme des coefficients de la colonne `j` de `A`.

7. Ecrire en pseudo-langage ou en `C++` une fonction `est_carré_magique(Matrice A)` qui retourne `true` si `A` est un carré magique et `false` sinon.

Exercice 3. Les éléments de $\mathbb{F}_2^n$ pourront être notés sous forme de n-uplets ou de vecteurs colonnes ou de mot de longueur n sur l'alphabet $\{0,1\}$. Soit φ le code correcteur défini par

$$\begin{array}{cccc} \varphi : & \mathbb{F}_2^2 & \to & \mathbb{F}_2^5 \\ & \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} & \mapsto & \begin{bmatrix} b_1 \\ b_2 \\ b_1+b_2 \\ b_2 \\ b_1 \end{bmatrix} \end{array}$$

1. Quel est le paramètre du code φ?

2. Quelle est l'image du code φ.

3. Quelle est la distance minimale de φ?

4. Quelles sont les capacités de détection et de correction pour φ ?

5. Le code φ est-il linéaire ? systématique ?

6. Le code φ est-il MDS ?

7. Donner la matrice génératrice de φ.

8. Donner une matrice de contrôle pour φ.

9. Calculer la table de décodage de φ.

10. Décoder les mots 01010 et 10011

Exercice 4. Soient $q = (2,2,0,1)$ et $q' = (-1,1,-1,1)$ deux quaternions.

1. Calculer $q + q'$.

2. Calculer $q \times q'$.

3. Calculer les normes de q et de q'.

4. Calculer q^* le conjugué de q.

5. Calculer q^{-1} l'inverse de q.

Exercice 5. Soient $P_0 = (-1,2)$, $P_1 = (0,1)$ et $P_2 = (1,-1)$ quatre points du plan. Le couple (x_i, y_i) désigne les coordonnées de P_i pour $i = 0,1,2$.

1. Calculer les polynômes $L_0(X), L_1(X)$ et $L_2(X)$ de $\mathbb{Q}[X]$ vérifiant

$$L_0(-1) = 1,\ L_0(0) = 0,\ L_0(1) = 0,\ L_1(-1) = 0,\ L_1(0) = 1,\ L_1(1) = 0,\ L_2(-1) = 0,\ L_2(0) = 0 \text{ et } L_2(1) = 1.$$

2. En déduire le polynôme $P(X)$ de $\mathbb{Q}[X]$ vérifiant $P(0) = 1$, $P(1) = 0$ et $P(2) = 2$.

Nous utilisons maintenant une spline quadratique

3. Rappeler la défintion d'une spline qudaratique.

On note q_0 et q_1 les polynômes constituant la spline quadratique d'interpolation de P_0, P_1 et P_2

4. Quelles sont les équations que doivent vérifier les polynômes q_i ?

Pour $i = 0,1$, on pose $q_i(x) = a_i(x - x_i)^2 + b_i(x - x_i) + c_i$

5. Quelles sont les équations que doivent satisfaire a_0, a_1, b_0, b_1, c_0 et c_1. ?

6. Quel est le nombre d'équations ? d'inconnues ? combien manque t-il d'équations ?

7. Calculer les valeurs $a_0, a_1, b_0, b_1, c_0, c_1$ puis les polynômes q_0 et q_1 en ajoutant la condition initiale $q_0'(x_0) = 0$.