Université du Littoral Côte d'Opale — Année universitaire 2010–2011
Licence 2ème année — Informatique

Courbes et Surfaces & Calcul formel

Documents et calculatrice autorisés.
3h le mercredi 18 mai 2011
Les réponses aux deux parties seront rédigés sur des copies différentes.

Toutes les réponses devront être justifiées.

I. Courbes et surfaces

Exercice 1. Trouver le polynôme $f\colon \mathbb{R} \to \mathbb{R}$ de degré 2 qui vérifie $f(0) = 3$, $f(1) = 2$ et $f(3) = -12$.

Exercice 2. Calculer la spline cubique naturelle $(q, p)\colon [0, 2] \to \mathbb{R}^2$ qui passe par les points $(x_0, y_0) = (0, 1)$, $(x_1, y_1) = (1, 3)$ et $(x_2, y_2) = (4, 2)$.

Exercice 3. Écrire la courbe polynomiale $\gamma\colon [0, 1] \to \mathbb{R}^2$,

$$\gamma(t) = \big(8t - 4t^3 - 2t^4, 1 - 16t + 42t^2 - 28t^3 + 5t^4\big),$$

comme courbe de Bézier (c'est-à-dire, identifier les points de contrôle $p = (p_0, \ldots, p_4)$) et dessiner sa trace. Dessiner aussi les étapes de l'algorithme de De Casteljau afin de déterminer $\gamma_B^p(3/4)$.

Exercice 4. Soit $p_0 = (-2, 0)$, $p_1 = (-1, 1)$, $p_2 = (0, 3)$ et $p_3 = (2, 1)$. Soit $\gamma_B^p\colon [0, 1] \to \mathbb{R}^2$ la courbe de Bézier associée.

(a) Dessiner γ_B^p.

(b) On veut prolonger γ_B^p par une courbe de Bézier γ_B^q qui finit en $q_3 = (0, -2)$ telle que la courbe composée de γ_B^p et γ_B^q soit de classe $\mathcal{C}^2$. Déterminer les points de contrôle q_0, q_1 et q_2. Dessiner γ_B^q dans le même plan cartesien que γ_B^p.

II. Calcul Formel

Exercice 5. [Chiffrement RSA] On pose $p = 3$ et $q = 7$ et $e = 5$

(a) Calculer $n = p \cdot q$ puis $\phi(n)$.

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

(c) Quels paramètres constituent la clé publique ? Et la clé privé e?

(d) Posons $M = 3$. Quel est le chiffré C de M.

(e) Retrouver M à partir de C et de la clé privée.

Exercice 6. [Polynôme] Notons E l'ensemble des polynômes à coefficents sur $\mathbb{Z}$ de degré inférieur ou égal à 9. On se propose de représenter un polynôme de E par :

```
struct{
 int coeffs[10];
}Poly;
```

Le polynôme $3x^8 + x^2 - 1$ aura alors le tableau `[-1,0,2,0,0,0,0,0,3,0]` comme `coeffs`.

(a) Ecrire une fonction `int degre(Poly P)` qui retourne le degré du polynome `P`.

(b) Ecrire une fonction `int eval(Poly P,int x)` qui retourne le polynôme `P` évalué en `x`.

(c) Ecrire une fonction `void racines(Poly P,int n)` qui affiche toutes les racines entières de `P` comprises entre `-n` et `n`.

(d) Ecrire une fonction `Poly deriv(Poly P)` qui retourne le polynôme dérivé de `P`.

(e) Un polynôme P a une racine multiple si le pgcd de P et P' est de degré au moins 1. On suppose que l'on a la fonction `Poly pgcd(Poly P,Poly Q)` retournant le pgcd de `P` et `Q`. Ecrire une fonction `int aUneRacineMultiple(Poly P)` retournant `1` si `P` a une racine multiple et `0` sinon.

Exercice 7. [Code correcteur] Soit ϕ le code correcteur de type (3.5) défini par :

$$\phi \begin{bmatrix} b_0 \\ b_1 \\ b_2 \end{bmatrix} = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_0 + b_2 \\ b_0 + b_1 + b_2 \end{bmatrix}$$

(a) Le code ϕ est-il linéaire ? Systématique ?

(b) Quelle est la matrice génératice de ϕ ?

(c) Quelle est la matrice de contrôle de ϕ ?

(d) Combien d'erreurs ϕ peut-il détecter ? Et corriger ?