

Contrôle du 17 janvier 2012

Sans documents. La rédaction sera notée : soyez précis et rigoureux.

Exercice 1 (2,5 pts)

1. Calculer 3^{129} [5]. 0,5 pt
2. Calculer 3^{129} [7]. 0,5 pt
3. En utilisant les calculs précédents calculer 3^{129} [35]. 1,5 pt

Exercice 2 (2,5 pts)

1. Soit $a \in (\mathbb{Z}/n\mathbb{Z})^*$ et un entier $k > 0$. Montrer que si $a^k = 1$ alors l'ordre de a divise k . 1 pt
2. Montrer que 9 est l'ordre de 2 modulo 511. 0,5 pt
3. En utilisant les questions précédentes répondre à la question :
511 est-il un nombre premier ? 1 pt

Exercice 3 (5 pts)

Soit $P(x)$ un polynôme dans $\mathbb{Q}[x]$ et $P'(x)$ sa dérivée.

Définition : α est une racine de multiplicité m de $P(x)$ si $P(x) = (x - \alpha)^m Q(x)$ et $Q(\alpha) \neq 0$.

1. Montrer que si α est une racine de multiplicité m de $P(x)$ alors α est une racine de multiplicité $m - 1$ de $P'(x)$. 1,5 pts
2. Quelles sont les racines et avec quelle multiplicité de $P(x)/\text{pgcd}(P(x), P'(x))$? 2,5 pts
3. Ceci est-il aussi vrai pour un polynôme dans $\mathbb{Z}/p\mathbb{Z}[x]$ avec p premier ? 1 pt

Exercice 4 (6 pts)

Soit le polynôme $F(x) = 1 + 2x^2 + 2x^3 + x^4$ dans $\mathbb{Z}/3\mathbb{Z}[x]$. On admet que $F(x)$ est sans facteur multiple.

On va travailler dans l'espace vectoriel $\mathbb{Z}/3\mathbb{Z}[x]/(F(x))$ représenté par les restes des polynômes de $\mathbb{Z}/3\mathbb{Z}[x]$ dans la division euclidienne par $F(x)$. Cet espace vectoriel admet pour base $1, x, x^2, x^3$ puisque $F(x)$ est de degré 4.

On considère l'application $\mathcal{B} : g(x) \rightarrow g^3(x) - g(x) \pmod{F(x)}$ de $\mathbb{Z}/3\mathbb{Z}[x]/(F(x))$ dans lui-même. Cette application est linéaire (voir le cours).

1. Calculer la matrice de \mathcal{B} dans la base $1, x, x^2, x^3$. 3 pts
2. Calculer une base du noyau de \mathcal{B} sous forme de polynômes. 2 pts
3. Combien $F(x)$ a-t-il de facteurs irréductibles ? Quels calculs faut-il faire pour les trouver ? 1 pt

Exercice 5 (4 pts)

Soit un polynôme $F(x)$ de degré n dans $\mathbb{Z}/p\mathbb{Z}[x]$, p premier.

L'espace vectoriel $\mathbb{Z}/p\mathbb{Z}[x]/(F(x))$ représenté par les restes des polynômes de $\mathbb{Z}/p\mathbb{Z}[x]$ dans la division euclidienne par $F(x)$ admet pour base $1, x, x^2, \dots, x^{n-1}$ puisque $F(x)$ est de degré n .

On considère l'application linéaire $\mathcal{B} : g(x) \rightarrow g^p(x) - g(x) \pmod{F(x)}$ de $\mathbb{Z}/p\mathbb{Z}[x]/(F(x))$ dans lui-même.

On suppose disposer d'une fonction Maple `PolyenVect:=proc(P,n) ... end` : qui convertit un polynôme $P(x)$ de degré au plus $n - 1$ en le vecteur de ses n coefficients.

Écrire la fonction Maple `MatriceB:=proc(F,p) ... end` : qui calcule la matrice de l'application linéaire \mathcal{B} dans la base $1, x, x^2, \dots, x^{n-1}$.