

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

Solution :

1. D'après Fermat $3^4 = 1$ [5] or $129 = 4 \times 32 + 1$ donc $3^{129} = (3^4)^{32} \times 3 = 3$ [5].
2. D'après Fermat $3^6 = 1$ [7] or $129 = 6 \times 21 + 3$ donc $3^{129} = (3^6)^{21} \times 3^3 = 27 = 6$ [7].

3. On cherche une solution de $\begin{cases} x = 3 & [5] \\ x = 6 & [7] \end{cases}$.

On calcule une relation de Bézout entre 5 et 7, par exemple $3 \times 5 - 2 \times 7 = 1$.

On a alors $x = 3 \times 5 \times 6 - 2 \times 7 \times 3$ [35] (Théorème des restes chinois). Soit $x = 90 - 42 = 48 = 13$ [35]. Comme la solution est unique modulo 35 on a $3^{129} = 13$ [35].

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

Solution :

1. On pose $d = \text{ordre}(a)$. On fait la division euclidienne de k par d , toujours possible puisque $d \neq 0$, $k = dq + r$ avec $0 \leq r < d$. Donc $a^k = (a^d)^q a^r = a^r = 1$ avec $0 \leq r < d$. D'après la définition de $\text{ordre}(a)$, le plus petit d non nul tel que $a^d = 1$, on a $r = 0$ et donc $k = dq$.
2. $2^9 = (2^3)^3 = 8^3 = 512 = 1$ [511] donc 9 est l'ordre ou un multiple de l'ordre de 2 modulo 511, or $2^3 = 8 \neq 1$ [511] donc 9 est l'ordre de 2 modulo 511.
3. Si 511 est un nombre premier $2^{510} = 1$ [511] (Fermat), donc 9 divise 510 (première question). Or $510 = 51 \times 10$, 9 et 10 sont premiers entre eux et $51 = 5 \times 9 + 6$ n'est pas divisible par 9 donc 510 n'est pas divisible par 9^1 donc 511 n'est pas premier.

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

¹On pouvait aussi faire la division euclidienne de 510 par 9 mais c'est moins amusant.

Solution :

- Si α est une racine de multiplicité m de $P(x)$ alors $P(x) = (x - \alpha)^m Q(x)$ avec $Q(\alpha) \neq 0$.
On a alors $P'(x) = m(x - \alpha)^{m-1} Q(x) + (x - \alpha)^m Q'(x) = (x - \alpha)^{m-1} (mQ(x) + (x - \alpha)Q'(x))$.
On pose $R(x) = mQ(x) + (x - \alpha)Q'(x)$.
On a $R(\alpha) = mQ(\alpha) + (\alpha - \alpha)Q'(\alpha) = mQ(\alpha) \neq 0$. Donc $P'(x) = (x - \alpha)^{m-1} R(x)$ et $R(\alpha) \neq 0$, c'est la définition de α est une racine de multiplicité $m - 1$ de $P'(x)$.
- Le polynôme $\text{pgcd}(P(x), P'(x))$ divise évidemment $P(x)$.
On a $P(x) = \text{pgcd}(P(x), P'(x))S(x)$ où $S(x) = P(x)/\text{pgcd}(P(x), P'(x))$.
Si α est une racine de $S(x)$ alors $S(\alpha) = 0$ donc $P(\alpha) = 0$, α est une racine de $P(x)$.
Soit α une racine de $P(x)$ de multiplicité m .
Alors $P(x) = (x - \alpha)^m Q(x)$ avec $Q(\alpha) \neq 0$ et $P'(x) = (x - \alpha)^{m-1} R(x)$ avec $R(\alpha) \neq 0$,
donc $\text{pgcd}(P(x), P'(x)) = (x - \alpha)^{m-1} \text{pgcd}((x - \alpha)Q(x), R(x))$.
Comme $R(\alpha) \neq 0$, $R(x)$ n'est pas divisible par $(x - \alpha)$ qui est un polynôme irréductible
donc $\text{pgcd}((x - \alpha)Q(x), R(x)) = \text{pgcd}(Q(x), R(x))$ et $\frac{P(x)}{\text{pgcd}(P(x), P'(x))} = \frac{(x - \alpha)^m Q(x)}{(x - \alpha)^{m-1} \text{pgcd}(Q(x), R(x))} = (x - \alpha) \frac{Q(x)}{\text{pgcd}(Q(x), R(x))}$ avec $Q(\alpha) \neq 0$.
Donc α est une racine de multiplicité 1 de $\frac{P(x)}{\text{pgcd}(P(x), P'(x))}$.
Les racines de $\frac{P(x)}{\text{pgcd}(P(x), P'(x))}$ sont les racines de $P(x)$ à la multiplicité 1.
- Non. Par exemple on prend dans $\mathbb{Z}/3\mathbb{Z}[x]$ le polynôme $P(x) = x^3 - 2 = (x - 2)^3$ [3], il a pour racine 2 à la multiplicité 3 et $P'(x) = 3x^2 = 0$ [3].
Les résultats des questions 1 et donc 2 ne sont pas vérifiées.

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).

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

Solution :

- On calcule les images des vecteurs de base par \mathcal{B} :

- L'image de 1 est le polynôme 0 donc le vecteur colonne $(0,0,0,0)$.
- L'image de x est le polynôme $x^3 - x = x^3 + 2x$ donc le vecteur colonne $(0,2,0,1)$.
- L'image de x^2 est le polynôme $x^6 - x^2 = x^6 + 2x^2 \pmod{F(x)}$. Il faut faire la division :

$$\begin{array}{r|l}
 x^6 + 2x^2 & x^4 + 2x^3 + 2x^2 + 1 \\
 - x^6 + 2x^5 + 2x^4 + x^2 & x^2 + x + 2 \\
 \hline
 x^5 + x^4 + x^2 & \\
 - x^5 + 2x^4 + 2x^3 + x & \\
 \hline
 2x^4 + x^3 + x^2 + 2x & \\
 - 2x^4 + x^3 + x^2 + 2 & \\
 \hline
 2x + 1 &
 \end{array}$$

On obtient comme reste $2x + 1$ donc le vecteur colonne $(1,2,0,0)$.

- L'image de x^3 est le polynôme $x^9 - x^3 = x^9 + 2x^3 \pmod{F(x)}$. Il faut faire la division mais on peut se servir des calculs précédents : $x^6 - x^2 = 2x + 1 \pmod{F(x)}$ donc $x^6 = x^2 + 2x + 1 \pmod{F(x)}$ donc $x^9 = x^5 + 2x^4 + x^3 \pmod{F(x)}$ et $x^9 - x^3 = x^5 + 2x^4 \pmod{F(x)}$, la division est plus simple :

$$- \frac{x^5 + 2x^4}{x^3 + 2x} \left| \frac{x^4 + 2x^3 + 2x^2 + 1}{x} \right.$$

On obtient comme reste $x^3 + 2x$ donc le vecteur colonne $(0,2,0,1)$.
On obtient finalement la matrice de \mathcal{B} :

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

2. On voit facilement qu'une base du noyau est $(1, x^3 + 2x)$: l'image des constantes est 0, l'image de x est la même que celle de x^3 donc l'image de $x^3 - x = x^3 + 2x$ est 0. L'image de x et celle de x^2 sont indépendantes, on a donc une image de dimension 2 et un noyau de dimension 2.
3. Le polynôme $F(x)$ a donc deux facteurs irréductibles. Pour les trouver il faut calculer $\text{pgcd}(F(x), x^3 + 2x)$, $\text{pgcd}(F(x), x^3 + 2x + 1)$ et $\text{pgcd}(F(x), x^3 + 2x + 2)$.

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 polynomes 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 $1, x, x^2, \dots, x^{n-1}$.

Solution :

```
MatriceB:=proc(F,p)
local n,k,Imxk,V;
n:=degree(F,x);
for k from 0 to n-1 do
  Imxk:=Rem(x^(p*k)-x^k,F,x) mod p;V[k]:=PolyenVect(Imxk,n)
od;
linalg[transpose](matrix([seq(V[k],k=0..n-1)]))
end;
```

On calcule les images des vecteurs de base x^k par l'application linéaire \mathcal{B} .

$\mathcal{B} : x^k \rightarrow x^{pk} - x^k \pmod{F(x)}$ qu'on convertit ensuite en vecteur dans les variables $V[k]$.

Le constructeur `matrix` à qui on donne la liste des $V[k]$ fabrique une matrice dont les *lignes* sont les $V[k]$. On la transpose pour obtenir la matrice dont les *colonnes* sont les $V[k]$.

Dans le corrigé du TP9 on trouve une version plus compliquée de cette fonction qui économise des calculs au cours de la boucle en se servant des résultats déjà calculés (mais ce n'était pas demandé).

Les variables `Imxk` et `V[k]` ne sont pas nécessaires. Elles servent à mieux comprendre les étapes du calcul et à ne pas vous traumatiser mais si vous aimez la programmation fonctionnelle très emboîtée on peut écrire :

```
MatriceB:=proc(F,p)
local n,k;
n:=degree(F,x);
linalg[transpose](matrix([seq(PolyenVect(Rem(x^(p*k)-x^k,F,x) mod p,n),k=0..n-1)]))
end:
```