EISTI
Ecole Internationale des Sciences du Traitement de l'Information

Département de Mathématiques
Année universitaire 2017-2018

CORRECTION DS3

Matière : **Algèbre**
Filière : **CPI1 - Pau**
Durée : **2h**
Responsable : **Barrau Nelly**

Q.C.M. 1 *[2,5 points]* Réponse exacte (0.25pt), Pas de réponse (0pt), Réponse fausse (-0.25pt).
Aucune justification n'est demandée. **[Réponses DIRECTEMENT écrites sur la copie]**

1. Soit P un polynôme non nul à coefficients réels. Parmi les affirmations suivantes, lesquelles sont vraies et lesquelles sont fausses :
   A : Le degré de $P((X+2)^2)$ est le double du degré de P. **VRAI**
   B : Le degré de $(X+2)P((X+2)^2)$ est toujours supérieurs ou égal à 2. **FAUX**
   C : Le degré de $P'((X+2)^2)$ est soit un entier impair, soit $-\infty$. **VRAI**
   D : Le degré de $(X+2)^2P'((X+2)^2)$ est toujours supérieur ou égal à 2. **FAUX**
   E : Le degré de $(X+2)^2P'((X+2)^2)$ est toujours le double du degré de P. **FAUX**
2. Soient $P, Q \in \mathbb{R}[X]$ deux polynômes non nuls. Parmi les affirmations suivantes, lesquelles sont vraies et lesquelles sont fausses :
   A : Les polynômes $P(Q)$ et $Q(P)$ ont toujours le même degré. **VRAI**
   B : Les polynômes PQ et $P(Q)$ ont toujours le même degré. **FAUX**
   C : Si le polynômes Q est constant, alors les polynômes PQ et $P(Q)$ ont le même degré. **FAUX**
   D : Si les polynômes $P+Q$ et PQ ont le même degré, alors au moins un des deux polynômes P et Q est constant. **VRAI**
   E : Si les polynômes PQ et $P(Q)$ ont le même degré, alors les deux polynômes P et Q sont constants. **FAUX**

Exercice 1 *[5 points]*
Soient $a, b \in \mathbb{N}^*$ fixés. On souhaite résoudre dans $\mathbb{N}^*$ le système d'équations :

$$(S) \begin{cases} x \wedge y &= a \\ x \vee y &= b \end{cases}$$

1. Montrer que sur a ne divise pas b, alors (S) n'admet pas de solution.
   Si a ne divise pas b, alors pour tout $(x,y) \in (\mathbb{N}^*)^2$, $x \wedge y$ ne divise pas $x \vee y$, ie $\mathcal{S} = \emptyset$ (car $x \wedge y$ divise nécessairement $x \vee y$).
2. Supposons que $a \mid b$. Exprimer la forme générale des solutions de (S).
   Supposons $a \mid b$, ie $\exists c \in \mathbb{N}^* : b = ac$.
   Soit $(x,y) \in (\mathbb{N}^*)^2$, posons $d = x \wedge y$. Alors $\exists X, Y \in \mathbb{N}^* : x = dX, y = dY$ et $X \wedge Y = 1$.Le système (S) se simplifie alors :

$$(S) \begin{cases} x \wedge y &= a \\ x \vee y &= b \end{cases} \iff \begin{cases} d &= a \\ dXY &= b = ac \end{cases} \iff \begin{cases} d &= a \\ XY &= c \end{cases}$$

   L'ensemble des solutions de (S) est donné par

$$\mathcal{S} = \left\{ (aX, aY) : X \mid c, Y = \frac{c}{X} \text{ et } X \wedge Y = 1 \right\}.$$

3. Application : Résoudre (S) dans les deux cas suivants :

(a) $a = 10$ et $b = 22$. On a clairement que a ne divise pas b. D'après la question 1., $\mathcal{S} = \emptyset$.

(b) $a = 8$ et $b = 80$. On a $a \mid b$ car $b = 80 = 8 \times 10 = 10a$. D'où :

$$(S) \begin{cases} x \wedge y &= 8 \\ x \vee y &= 80 \end{cases} \iff \begin{cases} d &= 8 \\ XY &= 10 \end{cases}$$

Il vient

$$\mathcal{S} = \left\{ (8X, 8Y) : X \mid 10, Y = \frac{10}{X} \text{ et } X \wedge Y = 1 \right\}.$$

En particuliers, X et Y sont des diviseurs de 10, ie $1, 2, 5$ et 10. Étudions les différents cas

$$\begin{cases} X &= 1 \\ Y &= \frac{10}{1} = 10 \end{cases} \text{ ou } \begin{cases} X &= 2 \\ Y &= 5 \end{cases} \text{ ou } \begin{cases} X &= 5 \\ Y &= 2 \end{cases} \text{ ou } \begin{cases} X &= 10 \\ Y &= 1 \end{cases}$$

D'où

$$\begin{cases} x &= 8X = 8 \\ y &= 8Y = 80 \end{cases} \text{ ou } \begin{cases} x &= 16 \\ y &= 40 \end{cases} \text{ ou } \begin{cases} x &= 40 \\ y &= 16 \end{cases} \text{ ou } \begin{cases} x &= 80 \\ y &= 8 \end{cases}$$

Finalement

$$\mathcal{S} = \{(8, 80); (16, 40); (40, 16); (80, 8)\}.$$

Exercice 2 *[5 points]* **Petit théorème de Fermat**

Soit p un nombre premier ($p \geq 2$).

I – **DÉMONSTRATION**

1. Soit $k \in \{1, ..., p-1\}$. Montrer que $p \mid \binom{p}{k}$. En déduire la congruence de $\binom{p}{k}$ modulo p.

   Par définition :

   $$\binom{p}{k} = C_p^k = \frac{p!}{k!(p-k)!} \iff \binom{p}{k} k!(p-k)! = p!$$

   Donc p divise $\binom{p}{k} k!(p-k)!$. Comme $1 \leq k \leq p-1$ et p est premier, on a $p \wedge (k!) = 1$ et $p \wedge ((p-k)!) = 1$, donc d'après le théorème de Gauss $p \mid \binom{p}{k}$. Ainsi $\binom{p}{k} \equiv 0\ [p]$.

2. Montrer par récurrence que $\forall n \in \mathbb{N}, n^p \equiv n[p]$.

   Indications : Cette récurrence s'effectue sur les n (p est premier et est fixé)! La formule du binôme de Newton et le résultat de la question 1. pourront être utiles.

   Posons la proposition G_n : "$n^p \equiv n[p]$".

   — **Initialisation** : la propriété est évidente pour $n = 0$.

   — **Hérédité** : Supposons pour $n \in \mathbb{N}$ fixé que G_n est vraie, ie $n^p \equiv n[p]$.
   Montrons que G_{n+1} est vraie, ie $(n+1)^p \equiv (n+1)[p]$.
   La formule du binôme de Newton nous dit que

   $$(n+1)^p = \sum_{k=0}^{p} C_p^k n^k 1^{p-k} = \sum_{k=0}^{p} C_p^k n^k = 1 + \sum_{k=1}^{p-1} C_p^k n^k + n^p$$

   Or d'après la question 1., $\forall k \in \{1, ..., p-1\}, p \mid C_p^k$. D'où

   $$(n+1)^p \equiv 1 + n^p\ [p] \iff (n+1)^p \equiv 1 + n\ [p] \quad \sharp \text{ car } n^p \equiv n[p]$$

   Ainsi G_{n+1} est vraie

   — **Conclusion** : $\forall n \in \mathbb{N}, n^p \equiv n[p]$.

Le résultat de la question 2 se généralise par $\forall n \in \mathbb{Z}, n^p \equiv n[p]$. Une conséquence directe de cette formule est :

" Si p ne divise pas n, alors $n^{p-1} \equiv 1[p]$. "

$II-$ APPLICATION

1. Calculer 3^{100} modulo 23.
   En utilisant le résultat, 23 étant un nombre premier et 23 ne divise pas 3, donc $3^{22} \equiv 1[23]$. De plus, $100 = 22 \times 4 + 12$. D'où

   $$3^{100} = 3^{22\times 4+12} = (3^{22})^4\, 3^{12} \equiv (1)^4 3^{12}\ [23]$$

   De plus, $3^{12} = (3^3)^4 = (27)^4 \equiv 4^4\ [23]$. Enfin $4^4 = 256 = 23 \times 11 + 3$.
   Ainsi $3^{100} \equiv 3\ [23]$.
2. Calculer 14^{3141} modulo 17.
   En utilisant le résultat, 17 étant un nombre premier et 17 ne divise pas 14, donc $14^{16} \equiv 1[17]$.
   De plus, $3141 = 16 \times 196 + 5$. D'où

   $$14^{3141} = 14^{16\times 196+5} = (14^{16})^{196}\, 14^5 \equiv (1)^{196} 14^5\ [17]$$

   De plus, $14^5 \equiv (-3)^5\ [17]$. Il vient donc $14^2 \equiv (-3)^2 = 9 \equiv 9\ [17]; 14^3 \equiv (-3)^3 = -27 \equiv 7\ [17]; 14^5 = 14^3 \times 14^2 \equiv 7 \times 9 = 63 \equiv 12\ [17]$.
   Ainsi $14^{3141} \equiv 12\ [17]$.

Exercice 3 *[5 points]*
Soient $A, B, C \in \mathbb{Z}^*$. On considère l'équation diophantienne :

$$(E) : Ax + By = C.$$

Résoudre (E) consiste à déterminer l'ensemble des solutions $\mathcal{S} = \{(x, y) \in \mathbb{Z}^2 : Ax + By = C\}$.

1. Posons $d = A \wedge B$. Montrer que si d ne divise pas C, alors $\mathcal{S} = \emptyset$.
   Par contraposée : Si $\mathcal{S} \neq \emptyset$, alors il existe $(x, y) \in \mathbb{Z}^2$ tels que $Ax + By = C$. Comme $d \mid A$ et $d \mid B$, il vient nécessairement que $d \mid C$.
2. Supposons $d \mid C$. Montrer que l'équation (E) a même ensemble de solutions que l'équation

   $$(E') : A'x + B'y = C'.$$

   On prendra soin de préciser le lien entre A, B, C et A', B', C'.
   Comme $d = A \wedge B$ et $d \mid C$, A, B, C sont donc divisibles par d : alors il existe $A', B', C' \in \mathbb{Z}$ tels que $A = dA'; B = dB'$ et $C = dC'$. L'équation (E) s'écrit alors

   $$(E) : d(A'x + B'y) = dC' \Longleftrightarrow (E') : A'x + B'y = C'$$

3. Comment trouver une solution particulière de l'équation (E') ?
   A' et B' sont premiers entre eux, donc d'après le théorème de Bezout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $A'u + B'v = 1$.
   On trouve (u, v) une solution particulière de $A'u + B'v = 1$, en remontrant l'algorithme d'Euclide.
   Alors $(C'u; C'v)$ est une solution particulière de (E').
4. En déduire l'ensemble $\mathcal{S}$ de toutes les solutions.
   On obtient (en utilisant le lemme de Gauss)

   $$\mathcal{S} = \{(C'u + B'k; C'v - A'k), k \in \mathbb{Z}\}.$$

5. Résoudre dans $\mathbb{Z}$ l'équation $24x + 20y = 36$.
   En appliquant la démonstration précédente, il vient $24 \wedge 20 = 4$ et $4 \mid 36$. Cette équation diophantienne admet donc des solutions dans $\mathbb{Z}$ et

$$(E) : 24x + 20y = 36 \iff (E') : 6x + 5y = 9.$$

   6 et 5 étant premier entre eux, d'après le théorème de Bezout, on sait qu'il existe $(u, v) \in \mathbb{Z}^2$ tels que $6u + 5v = 1$. On remarque qu'un solution particulière de cette équation est $(1; -1)$. Donc une solution particulière de (E') est $(9; -9)$. L'ensemble des solutions de (E) est donné par

$$\mathcal{S} = \{(9 + 5k; -9 - 6k), k \in \mathbb{Z}\}.$$

Exercice 4 *[2,5 points]*
Soient $A, B \in \mathbb{K}[X]$ définis par

$$A = X^4 + 2X^2 - 3X^3 - 2X + 4 \qquad B = X^2 + 1$$

1. Effectuer la division euclidienne de A par B.

$A =$	X^4	$-3X^3$	$+2X^2$	$-2X$	$+4$	X^2+1	$= B$
$-$	$(X^4$		$+X^2)$			X^2-3X+1	$= Q$
		$-3X^3$	$+X^2$	$-2X$	$+4$		
	$-$	$(-3X^3$		$-3X)$			
			X^2	$+X$	$+4$		
		$-$	$(X^2$		$+1)$		
			$R =$	X	$+3$		

   Ainsi : $A = B(X^2 - 3X + 1) + (X + 3)$.

2. Calculer $A \wedge B$.
   D'après la division précédente : $A \wedge B = B \wedge (X + 3)$. On effectue de nouvelles divisions euclidiennes, jusqu'à obtenir un reste nul :

$$\begin{aligned} B &= (X+3) \times (X-3) + 10 \qquad \rightsquigarrow B \wedge (X+3) = (X+3) \wedge 10 \\ (X+3) &= 10 \times \left(\tfrac{1}{10}X + \tfrac{3}{10}\right) + 0 \end{aligned}$$

   On rappelle que le pgcd entre polynômes est un polynôme normalisé : le polynôme normalisé de 10 est 1. Ainsi $A \wedge B = B \wedge (X + 3) = (X + 3) \wedge 10 = 1$.

3. Effectuer la division à l'ordre 3 de A par B.

$A =$	4	$-2X$	$+2X^2$	$-3X^3$	$+X^4$		$1+X^2$	$= B$
$-$	$(4$		$+4X^2)$				$4-2X-2X^2-X^3$	$= Q$
		$-2X$	$-2X^2$	$-3X^3$	$+X^4$			
	$-$	$(-2X$		$-2X^3)$				
			$-2X^2$	$-3X^3$	$+X^4$			
		$-$	$(-2X^2$		$-2X^4)$			
				$-X^3$	$+3X^4$			
			$-$	$(-X^3$		$-X^5)$		
					$3X^4$	$+X^5$		

   Ainsi : $A = B(4 - 2X - 2X^2 - X^3) + X^4(3 + X)$.

Exercice 5 *Bonus [2 points]*
Résoudre dans $\mathbb{Z}$ l'équation $18x^2 - 31x + 11 \equiv 0[7]$.
En procédant à une première simplification :

$$18x^2 \equiv 4x^4 \ [7] \qquad -31x \equiv -3x \ [7] \qquad 11 \equiv -3 \ [7]$$

On cherche donc à résoudre dans $\mathbb{Z}$: $4x^2 - 3x \equiv -3 \ [7]$. On peut effectuer un tableau récapitulatif :

x	0	1	2	3	4	5	6
$4x^2$	0	4	2	1	1	2	4
$3x$	0	3	6	2	5	1	4
$4x^2 - 3x$	0	1	3	6	3	1	0

Ainsi, l'ensemble des solutions de l'équation proposée est l'ensemble des entiers congrus à 2 ou à 4 modulo 7.
Remarque : la résolution pouvait se faire littéralement : $18x^2 - 31x \equiv -11[7]$ peut s'écrire :

$$18x^2 \equiv 4x^4 \ [7] \qquad -31x \equiv -3x \equiv 4x \ [7] \qquad -11 \equiv 3 \equiv -4 \ [7]$$

Alors

$$18x^2 - 31x \equiv -11[7] \iff 4x^2 + 4x \equiv -4 \ [7] \iff x(x+1) \equiv -1 \equiv 6 \ [7]$$

On cherche donc x tel que le produit des deux nombres consécutifs x et $x+1$ est congru à 6 ou -1. Pour 6, on a $2 \times 3 = 6$, donc $x \equiv 2 \ [7]$ est solution. Et $4 \times 5 = 20 = 21 - 1 \equiv -1 \ [7]$. donc $x \equiv 4 \ [7]$ est également solution.