Approfondissement

Solutions

Exercice 1.

1. Quels sont les ordres multiplicatifs de 2 mod 3, mod 7, mod 9 et mod 19 ?

   Solution :
   Modulo 3, on a $2^n = (-1)^n$ de sorte que 2 est d'ordre 2 modulo 3
   Modulo 7, l'ordre de 2 est égal à 3.
   Modulo 9, on a $2^3 = -1 \mod 9$ et donc 2 est d'ordre 6.
   Modulo 19, les ordres possibles de 2 étant les diviseurs de 18 on peut tous les tester. On a que 2 n'est pas d'ordre 2 ni d'ordre 9 car $2^9 = -1 \mod 19$, donc 2 est d'ordre 18 modulo 19.

2. Montrer que si n est un entier impair, alors 7 divise $2^{2^n} + 3$.

   Solution : Si n est impair, on a $2^n = 2 \mod 3$ et de sorte que, d'après la premiére question, $2^{2^n} = 2^2 \mod 7$ et donc $2^{2^n} + 3$ est divisible par 7.

3. Montrer que si $n \equiv 2 \mod 6$, alors 19 divise $2^{2^n} + 3$.

   Solution : D'après le lemme chinois, comme 2^n est stationnaire modulo 2 et périodique de période 6 modulo 9, on en déduit qu'elle est périodique de période 6 modulo $18 = 2 \times 9$.
   D'après cela, la congruence modulo 19 de $2^{2^n}+3$ ne dépend que de la congruence de $2^n \mod 18$ (car l'ordre de 2 est 18) et donc de la congruence de $n \mod 6$ de sorte que pour $n \equiv 2 \mod 6$, on a $2^{2^n} = 2^4 \mod 19$ et donc 19 divise $2^{2^n} + 3$.

Exercice 2.

1. Déterminer le nombre d'éléments de l'anneau $\mathbb{A} = \mathbb{F}_5[X]/(X^2 + 4)$.

   Solution : $|\mathbb{A}| = 5^2$.

2. Justifier si la classe du polynôme $X^3 + 2X^2 - X + 2$ est inversible dans $\mathbb{A}$. Dans le cas échéant, calculer son inverse.

   Solution : Si le polynôme $X^3 + 2X^2 - X + 2$ est prémier avec $X^2 + 4$, alors il est un élément inversible de $\mathbb{A}$.

   Méthode 1 :
   La classe du polynôme P est le reste du division de P avec Q. Le reste R étant 4, on a que la classe de 4 dans (le corps des coefficients) $\mathbb{Z}/5\mathbb{Z}$ est inversible, donc l'inverse du 4 dans $\mathbb{Z}/5\mathbb{Z}$ coïncide avec l'inverse du P dans $\mathbb{A}$.

Méthode 2 :
On calcule avec l'algorithme d'Euclide le pgcd de $P = X^3 + 2X^2 - X + 2$ et $Q = X^2 + 4$ et on obtient le dernier reste non-nul $d = 4$.
On utilise la Définition 5.3 du polycopié (page 80).
Très important ! Le pgcd doit être ***unitaire*** (l'unique polynôme unitaire qui satisfait la relation demandée). Dans notre cas, la classe de d=4 est un élément inversible de $\mathbb{Z}/5\mathbb{Z}$, donc l'unique polynôme unitaire dans l'idéal $I = (d)$ est $1 = dd^{-1}$, donc pgcd = 1. (Le seul polynôme de degré 0 unitaire est 1.)
Nous pouvons en déduire que les deux polynômes sont premiers entre eux

Méthode 3 :
Ou on peut directement appliquer le Corollaire 5.2 (page 81) en écrivant une relation de Bézout pour 4 :
$PU + QV = 4$ qu'on peut multiplier par l'inverse de 4 dans $\mathbb{Z}/5\mathbb{Z}$.
On obtient finalement une identité du type : $P \cdot 4U + Q \cdot 4V = 16 \equiv 1 \mod 5$.
Pour $U' = 4U$ et $V' = 4V$ on trouve la relation nécessaire pour appliquer le Corollaire 5.2 et conclure.

3. L'anneau $\mathbb{A}$ est-il un corps ? Pourquoi ?

   Solution : Le polynoôme $X^2 + 4$ a une racine dans $\mathbb{F}_5$ (la classe de 1 est racine), alors il est réductible :

$$X^2 + 4 = X^2 - 1 = (X - 1)(X + 1).$$

   Donc $\mathbb{A}$ n'est pas un corps.

Exercice 5. On considère l'ensemble $\mathbb{Z}[\sqrt{2}i] = \{a + b\sqrt{2}i | a, b \in \mathbb{Z}\}$

1. Montrer que $\mathbb{Z}[\sqrt{2}i]$ est un anneau commutatif intégre.

   Solution : On peut montrer que $\mathbb{Z}[\sqrt{2}i]$ est un anneau commutatif intègre de plusieurs façons différentes. En utilisant directement la déffinition ou bien on montre facilement que $\mathbb{Z}[\sqrt{2}i]$ est un sous-anneau de $\mathbb{C}$.

2. Pour tout nombre complexe $\alpha = x + yi$, on considère sa norme $N(\alpha) = x^2 + y^2$. Montrer que si $z_1, z_2 \in \mathbb{C}$, alors $N(z_1 z_2) = N(z_1)N(z_2)$.

   Solution : Si on note $z_1 = x_1 + iy_1$ et $z_2 = x_2 + iy_2$ on a :
   $N(z_1 z_2) = (x_1 x_2 - y_1 y_2)^2 + (y_1 x_2 + x_1 y_2)^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2) = N(z_1)N(z_2)$.

3. Montrer que tout idéal de $\mathbb{Z}[\sqrt{2}i]$ est principal.

   Solution : Soit I un idéal de $\mathbb{Z}[\sqrt{2}i]$. Si $I = \{0\}$, alors $I = (0)$. Sinon, soit $\alpha \in I$ un élément de norme minimale non nulle. Montrons que $I = \{\alpha z | z \in \mathbb{Z}[\sqrt{2}i]\}$.
   Par définition d'idéal, tout multiple de α est bien dans I.
   Réciproquement, montrons que tous les éléments de I sont des multiples de α. Soit $\beta \in I$ et effectuons la division euclidienne de β par α. Si le reste est non nul, par définition, sa norme est inferieure à la norme de α, ce qui conduit à une cotradiction, car α est censé d'être de norme minimale. Cela nous permet de conclure.