Feuille d'exercices n°2

Pgcd, ppcm, théorèmes de Bezout, Gauss, décomposition, congruences

---

Exercice 1.

1) Écrire l'algorithme d'Euclide dans $\mathbb{Z}$ pour $a = 693$ et $b = 294$. En déduire un pgcd de a et b, et une relation de Bezout entre a et b. Déterminer tous les pgcd de a et b.
2) Écrire l'algorithme d'Euclide dans $\mathbb{R}[X]$ pour $a = X^4 - 1$ et $b = X^2 - 3X + 2$. En déduire un pgcd de a et b, et une relation de Bezout entre a et b. Déterminer tous les pgcd de a et b.

Exercice 2. Montrer que les polynômes $X^4 + 1$ et $X^3 + 1$ sont premiers entre eux dans $\mathbb{R}[X]$.

Exercice 3. Donner la décomposition en facteurs premiers de :

1) dans $\mathbb{Z}$: 294 ; 693 ; 23 ; 350 ;
2) dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$: $X^2 - 3X + 2$; $X^4 - 2X^2 - 3$; $X^4 - 1$; $X^3 - X^2 - 2X + 2$; $\frac{1}{2}X^4 - 1$; $X^6 + 9X^4 + 27X^2 + 27$.

Exercice 4. Calculer les pgcd et les ppcm suivants :

1) dans $\mathbb{Z}$: $\text{pgcd}(294, 693)$; $\text{pgcd}(693, 350)$; $\text{pgcd}(294, 350)$; $\text{ppcm}(294, 693)$; $\text{ppcm}(693, 350)$; $\text{ppcm}(294, 350)$;
2) $\text{pgcd}(X^2 - 3X + 2, X^4 - 1)$ dans $\mathbb{Q}[X]$;
3) $\text{pgcd}(X^4 - 2X^2 - 3, X^4 - 1)$ dans $\mathbb{R}[X]$;
4) $\text{ppcm}(X^2 - 3X + 2, X^4 - 1)$ dans $\mathbb{Q}[X]$.

Démontrer que 693 et 25 sont premiers entre eux. Démontrer que $X^2 - 3X + 2$ et $X^4 - 2X^2 - 3$ sont premiers entre eux dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

Exercice 5.

1) Rappeler la forme générale des idéaux de $\mathbb{Z}$ et de $K[X]$ ($K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$).
2) Écrire les idéaux suivants sous la forme $n\mathbb{Z}$:
   a) $2\mathbb{Z} + 5\mathbb{Z}$ e) $2\mathbb{Z} \cap 6\mathbb{Z}$
   b) $294\mathbb{Z} + 693\mathbb{Z}$ f) $294\mathbb{Z} \cap 350\mathbb{Z}$
   c) $350\mathbb{Z} + 693\mathbb{Z}$ g) $693\mathbb{Z} \cap 350\mathbb{Z}$.
   d) $693\mathbb{Z} + 25\mathbb{Z}$
3) Écrire les idéaux suivants sous la forme $P(X)K[X]$:
   a) $(X - 1)\mathbb{R}[X] + (X + 3)\mathbb{R}[X]$
   b) $(X^2 - 3X + 2)\mathbb{Q}[X] + (X^4 - 1)\mathbb{Q}[X]$
   c) $(X^4 - 2X^2 - 3)\mathbb{R}[X] + (X^4 - 1)\mathbb{R}[X]$

d) $(X^2-3X+2)\mathbb{Q}[X] \cap (X^4-1)\mathbb{Q}[X]$.

4) *(Examen de juin 2003).* Déterminer tous les entiers positifs k satisfaisant à $1428\mathbb{Z} + 728\mathbb{Z} \subset k\mathbb{Z}$.

Exercice 6. Soit $n \in \mathbb{N}$, $n \geq 2$ et $n = p_1^{\alpha_1} \dots p_N^{\alpha_N}$ sa décomposition en produit de nombres premiers. Exprimer le nombre de diviseurs positifs de n en fonction de $\alpha_1, \dots, \alpha_N$.

Exercice 7. Démontrer que $\sqrt{2}$ est irrationnel.

CONGRUENCES

Exercice 8. Résoudre dans $\mathbb{Z}$ les équations suivantes :

1) $x \equiv 6 \mod 44$;

2) $x - 27 \equiv 18 \mod 44$.

Exercice 9. Démontrer à l'aide des congruences que 11 divise $2^{6n+3} + 3^{2n+1}$ pour tout $n \in \mathbb{N}$.

Exercice 10. Démontrer à l'aide des congruences que pour tout $a \in \mathbb{Z}$, le reste de la division euclidienne de a^2 par 8 est 0, 1 ou 4. En déduire que si $n \in \mathbb{N}$ est congru à 7 modulo 8, n ne peut être somme de trois carrés d'entiers.

Exercice 11. *On s'intéresse aux équations de la forme* $ax \equiv 1 \mod b$, *où* $(a,b) \in \mathbb{Z}^* \times \mathbb{Z}^*$, *d'inconnue* $x \in \mathbb{Z}$.

1) Résoudre $2x \equiv 1 \mod 4$ dans $\mathbb{Z}$.

2) Résoudre $2x \equiv 1 \mod 3$ dans $\mathbb{Z}$. On peut procéder de la façon suivante :
   - écrire une relation de Bezout entre 2 et 3 ;
   - en déduire une solution x de l'équation ;
   - soit x' une autre solution ; montrer qu'il existe $\lambda \in \mathbb{Z}$ tel que $x' = x + 3\lambda$ (penser au théorème de Gauss) ;
   - en déduire l'ensemble des solutions.

3) Résoudre $37x \equiv 1 \mod 44$. Résoudre $37y \equiv 2 \mod 44$.

4) *(Partiel de mars 2003).* Résoudre les équations suivantes :
   a) $71x \equiv 1 \mod 478$
   b) $717x \equiv 1 \mod 478$.

Exercice 12. Soit N un entier naturel et $N = a_0 + a_1 10 + \dots + a_p 10^p$ son écriture en base 10 (avec $a_0, \dots, a_p \in \mathbb{N}$).

1) Montrer que N est congru modulo 9 à la somme de ses coefficients $a_0, \dots, a_p$. En déduire un critère de divisibilité par 9.

2) L'entier 6210 est-il divisible par 9 ? L'entier 3759 est-il divisible par 9 ? Quel est son reste dans la division euclidienne par 9 ?

Exercice 13. Quel est le dernier chiffre de 7^{7^7} ?

Exercice 14. Déterminer le reste de la division euclidienne de $3548^9 \times 2537^{31}$ par 10.