Feuille d'exercices n°3

Congruences, théorème de Fermat, systèmes de congruences, racines de polynômes

---

Congruences, théorème de Fermat

Exercice 1. Quel est le dernier chiffre de 7^{30} ? Quel est le dernier chiffre de 7^{7^7} ?

Exercice 2. Déterminer le reste de la division euclidienne de 6^{1601} par 13. Déterminer le reste de la division euclidienne de $16^{2^{1000}}$ par 7.

Exercice 3. *(Partiel de mars 2003).* Soit q un nombre premier avec 3,5 et 17. On pose $a = q^{16} - 1$.

1) Démontrer que a est un multiple de 3, 5 et 17.
2) *(question intermédiaire)* Démontrer que si x, y, z sont des entiers tels que x divise z, y divise z, et x et y premiers entre eux, alors xy divise z (utiliser le théorème de Gauss).
3) Démontrer que a est un multiple de 255.

Equations ax+by=c

Exercice 4.

1) Soit $A = \mathbb{Z}$ ou $K[X]$ ($K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$). Soient $a, b, c \in A$ non nuls. Démontrer que l'équation $ax + by = c$ admet (au moins) une solution (x, y) dans $A \times A$ si et seulement si pgcd(a, b) divise c.
2) Déterminer tous les entiers relatifs x, y tels que :
   - a) 7x-9y=1
   - b) 7x-9y=6
   - c) 27x+15y=2
   - d) 27x+15y=3
   - e) 27x+15y=6
   - f) 1665x+1035y=8
   - g) 1665x+1035y=45
   - h) 20x + 30y=0
3) *(Examen de septembre 2003)* On pose $a = 2093$ et $b = 1365$. Déterminer un pgcd de a et b. Déterminer tous les couples $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tels que $ax + by = 182$.
4) On pose $A = X^8 - 1$ et $B = X^3 - 1$ dans $\mathbb{R}[X]$. Déterminer un pgcd D de A et B et un couple (U, V) de $\mathbb{R}[X]$ tels que $AU + BV = D$. En déduire tous les couples solutions de $AU + BV = D$.

Systèmes de congruences

Exercice 5. Résoudre les systèmes suivants :

$$\begin{cases} x \equiv 1 \mod 9 \\ x \equiv 2 \mod 7 \end{cases} \qquad \begin{cases} x \equiv 2 \mod 88 \\ x \equiv 1 \mod 27 \end{cases} \qquad \begin{cases} x \equiv 2 \mod 10 \\ x \equiv 5 \mod 6 \end{cases} \qquad \begin{cases} x \equiv 4 \mod 3 \\ x \equiv 1 \mod 6 \end{cases}$$

$$\begin{cases} 5x \equiv 4 \mod 7 \\ 4x \equiv 1 \mod 9 \end{cases}$$

Exercice 6. Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or. Ils décident de se les partager également, et de donner le reste au cuisinier. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Le cuisinier recevrait alors 4 pièces. Dans un naufrage ultérieur, seuls le butin, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Racines de polynômes

Exercice 7. On définit les polynômes suivants : $P(X) = X^3 - 3X^2 + 3X - 3$ et $Q(X) = X^4 - X^3 - 3X^2 + 3X - 4$.

1) Montrer que $x_0 = 1 + \sqrt[3]{2}$ est une racine de P.
2) En déduire la valeur de Q en x_0.

Exercice 8. Démontrer qu'il n'existe aucun polynôme $P \in \mathbb{R}[X]$ dont $x \mapsto \sin(x)$ soit la fonction polynôme associée.

Exercice 9. Les polynômes suivants ont-ils des racines doubles dans $\mathbb{R}$? dans $\mathbb{C}$?

1) $P(X) = (X - 27)^2(X + 41)$;
2) $Q(X) = (X^2 + 2)(X - i\sqrt{2})(X - \sqrt[3]{5})$;
3) $R(X) = X^3 + 3X^2 + 3X + 1$.

Exercice 10. *Les polynômes d'interpolation de Lagrange.* Soient $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, et n un entier positif. Soient $a_0, \ldots, a_n$ des éléments de K distincts deux à deux. Soient $\lambda_0, \ldots, \lambda_n \in K$ fixés. Nous allons démontrer le résultat suivant : il existe un unique polynôme $P \in K[X]$ de degré au plus n vérifiant : $P(a_0) = \lambda_0, \ldots, P(a_n) = \lambda_n$.

1) (Existence) On définit le polynôme suivant pour tout $i \in \{0, \ldots, n\}$:

$$L_i(X) = \frac{(X - a_0) \ldots (X - a_{i-1})(X - a_{i+1}) \ldots (X - a_n)}{(a_i - a_0) \ldots (a_i - a_{i-1})(a_i - a_{i+1}) \ldots (a_i - a_n)} \in K[X].$$

Quel est le degré de L_i ? Calculer $L_i(a_i)$ et $L_i(a_j)$ pour $j \neq i$. Démontrer que $P = \sum_{i=0}^{n} \lambda_i L_i$ est solution du problème posé.

2) (Unicité) Soient P_1 et P_2 deux solutions du problème. Démontrer que $P_1 = P_2$.

Exercice 11. Soit $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Pour $P = \sum_{k=0}^{n} a_k X^k$, on définit le polynôme dérivé $P' = \sum_{k=1}^{n} k a_k X^{k-1}$, puis $P^{(2)} = (P')', \ldots, P^{(s+1)} = (P^{(s)})'$.

1) Démontrer que l'application $D : P \mapsto P'$ de $K[X]$ dans $K[X]$ est K-linéaire.
2) Démontrer que les $P \in K[X]$ tels que $P' = 0$ forment un sous-espace vectoriel, formé des polynômes constants.
3) Démontrer la formule : pour tout $n \in \mathbb{N}$, $(PQ)^{(n)} = \sum_{k=0}^{n} \mathrm{C}_n^k P^{(k)} Q^{(n-k)}$.
4) Démontrer que pour tout $s, n \in \mathbb{N}$, $s \leq n$ et $\gamma \in K$,

$$[(X + \gamma)^n]^{(s)} = n(n-1) \ldots (n - (s+1))(X + \gamma)^{n-s}.$$