L3 Alg effective TD 4

31 octobre, 14,21 novembre, 5 décembre 2016

Exemples d'équations linéaires sur $\mathbb{Z}$, méthode matricielle

1.a. Trouver $d \in \mathbb{Z}$ tel que $24\mathbb{Z} + 18\mathbb{Z} + 12\mathbb{Z} = d\mathbb{Z}$

b. Résoudre dans $\mathbb{Z}$ l'équation $24x + 18y + 12z = 12$.

c. Calculer la fome de Smith de la matrice $(24\ 18\ 12) \in \mathrm{M}_{1,3}(\mathbb{Z})$. Retrouver les solutions de la question b.

2. Calculer la forme de Smith de la matrice $(30\ 42\ 105) \in \mathrm{M}_{1,3}(\mathbb{Z})$. En déduire toutes les relations de Bezout pour la famille d'entiers $(30, 42, 105)$

3. Calculer la forme de Smith (avec les matrices de changement de bases) de la matrice

$$\begin{pmatrix} 3 & 6 \\ 6 & 2 \end{pmatrix}$$

puis résoudre le système :

$$\begin{cases} 3x + 6y & = & -3 \\ 6x + 2y & = & 4 \end{cases}$$

4. Soient $e_1, \dots, e_n$ n vecteurs de $\mathbb{Z}^n$ dont on note $[e_i]$ le vecteur colonne des coordonnées (dans la base canonique). Montrer que les trois conditions suivantes sont équivalentes :

1. $(e_1, \dots, e_n)$ est une base de $\mathbb{Z}^n$
2. La matrice $([e_1] \cdots [e_n])$ est inversible dans $\mathrm{M}_n(\mathbb{Z})$
3. $\det([e_1] \cdots [e_n]) = \pm 1$

5. Peut on compléter la famille formée du seul vecteur $(6, 10, 20, 15)$ en une base de $\mathbb{Z}^4$?
Si oui, exhiber une telle base et écrire les coordonnées du vecteur $(0, 1, 2, 3)$ dans cette base.
Qu'en est il du vecteur $(6, 10, 20)$ dans $\mathbb{Z}^3$?

6.a Soient $A \in \mathrm{M}_{p,q}(\mathbb{Z})$, K le noyau de l'application linéaire $\mathbb{Z}^q \to \mathbb{Z}^p$ de matrice A, L le noyau de l'application linéaire $\mathbb{Q}^q \to \mathbb{Q}^p$ de matrice A.
Montrer les propriétés suivantes :

1. $K \subset L$ pour l'inclusion naturelle de $\mathbb{Z}^q$ dans $\mathbb{Q}^q$.
2. Un vecteur de L est dans K si et seulement si il est à coefficients entiers.
3. Pour tout $x \in L$, il existe un entier $d \neq 0$ tel que dx est dans K.
4. Toute $\mathbb{Z}$-base de K est une $\mathbb{Q}$-base de L.
5. Soit $(e_1, \dots, e_r)$ une famille de K qui est une $\mathbb{Q}$-base de L. Alors $(e_1, \dots, e_r)$ est une $\mathbb{Z}$-base de K si et seulement si la forme de Smith de la matrice des coordonnées des e_i n'a que des 1 sur la diagonale.

b. Un algorithme rend la famille de solutions $((-1, 2, 0), (-1, 0, 2))$ à l'équation homogène $2x + y + z = 0$.
Montrer que cette famille est une base des solutions de l'équation sur $\mathbb{Q}$. Est-ce une base des solutions de l'équation sur $\mathbb{Z}$?

Relations de congruence, lemme chinois

7. Soient m, n deux entiers. Montrer que les conditions suivantes sont équivalentes :

a. L'application $\mathbb{Z}/mn \to \mathbb{Z}/m \times \mathbb{Z}/n, \quad x[mn] \mapsto (x[m], x[n])$ est un isomorphisme d'anneaux

b. L'application $\mathbb{Z} \to \mathbb{Z}/m \times \mathbb{Z}/n, \quad x \mapsto (x[m], x[n])$ est surjective

c. L'application $\mathbb{Z}^3 \to \mathbb{Z}^2, \quad (x, q_1, q_2) \mapsto (x + q_1 m, x + q_2 n)$ est surjective

Soient a, b deux entiers. A quelle condition sur m, n existe t-il un entier x tel que $x = a[m]$ et $x = b[n]$? Pouvez vous expliciter un tel x lorsqu'il existe ?

8. Soit n un entier premier distinct de 2. Que peut on dire de l'ordre de 2 dans le groupe multiplicatif $\mathbb{Z}/n^\times$? Que se passe t-il si n est un produit de nombres premiers distincts de 2 sans facteur carré ? Trouver par un algorithme Sagemath les trois premiers nombres premiers n tels que 2 soit d'ordre $n-1$ dans $\mathbb{Z}/n^\times$.

Supposons maintenant n premier distinct de $2, 5$. Comment se comparent l'ordre de 10 et les ordres de 2 et 5 dans $\mathbb{Z}/n^\times$?

9. Soit n un entier premier distinct de $2, 5$. Quel lien y a t-il entre l'ordre de 10 dans $\mathbb{Z}/n^\times$ et la longueur de la période dans le développement décimal de $\frac{1}{n}$?

Expérimenter par un algorithme Sagemath.