Université de Bordeaux
Mathématiques

Algèbre et calcul formel – Master
Année 2017–2018

FEUILLE D'EXERCICES n° 7

Travail sur machine
PGCD, relation de Bézout, théorème des restes chinois

Exercice 1 – [Commandes pour le pgcd]

1) Essayer les commandes

```
gcd(75,198)
xgcd(75,198)
```

Cette dernière commande donne un triplet (d, u, v). Vérifier que $d = 75u + 198v$. On peut aussi calculer le pgcd de plus de deux entiers en même temps.

```
gcd([75,198,220])
```

Mais si on remplace `gcd` par `xgcd` dans la commande précédente, on n'obtient pas de résultat. Nous écrirons une fonction pour cela dans l'exercice suivant.

2) Ces commandes `gcd` et `xgcd` fonctionnent aussi sur les polynômes.

a) Définir l'anneau $\mathbb{Q}[x]$ et calculer $\text{pgcd}(x^7 - 1, 2x^3 + 5x^2 - 7)$, ainsi que les coefficients de Bézout associés. Vérifier la relation de Bézout correspondante.

b) Même exercice avec $\text{pgcd}(x^7 - 1, x^3 - x^2 + 1)$. La classe de $x^3 - x^2 + 1$ dans $\mathbb{Q}[x]/(x^7 - 1)$ est-elle inversible ? Si tel est le cas, quelle est son inverse ?

c) Même exercice dans $\mathbb{F}_7[x]$ avec $\text{pgcd}(x^7 - x, x^4 + x^2 - 2)$, puis $\text{pgcd}(x^7 - x, x^4 + x^2 + 1)$.

Exercice 2 – [Relation de Bézout pour plus de deux entiers]

Comme on l'a vu ci-dessus, le logiciel sage permet de calculer le pgcd de deux entiers à l'aide de la commande `gcd`. La commande `xgcd` donne en plus les coefficients de Bézout. On a vu aussi que la commande `gcd([a1,...,an])` donne $\text{pgcd}(a_1, \ldots, a_n)$, mais que par contre, `xgcd([a1,...,an])` ne donne rien.

En utilisant `xgcd`, écrire un algorithme qui prend en entrée une famille d'entiers $(a_1, \ldots, a_n)$ et donne en sortie $d = \text{pgcd}(a_1, \ldots, a_n)$ et $(u_1, \ldots, u_n) \in \mathbb{Z}^n$ tel que

$$\sum_{i=1}^{n} a_i u_i = d.$$

Exercice 3 – [Un peu de calcul matriciel]

Dans l'exercice 4, on étudie la résolution dans $\mathbb{Z}^n$ d'une équation $a_1x_1 + \cdots + a_nx_n = b$. Pour cela, nous utiliserons un peu de calcul matriciel. C'est pourquoi cet exercice donne quelques commandes sage pour de tels calculs.

1) On peut définir un vecteur et une matrice de la manière suivante.

```
w = vector([1,1,-4])
A = matrix([[1,2,3],[3,2,1],[1,1,1]]); A
```

Remarquons d'abord que les indices commencent à 0. Si l'on tape `A[0,0]`, on obtient `1`.

2) Exécuter les commandes

```
A.det()
A*w
w*A
parent(A)
parent(w)
```

3) On peut aussi commencer par définir l'espace matriciel où se trouveront les matrices. Exécuter les commandes

```
EM=MatrixSpace(ZZ,3)
EV=VectorSpace(ZZ,3)
```

Erreur ! C'est que $\mathbb{Z}$ n'est pas un corps, on ne peut donc pas définir d'espace vectoriel sur $\mathbb{Z}$. On peut écrire à la place

```
EV=VectorSpace(QQ,3)
```

ou bien définir le module $\mathbb{Z}^3$ sur $\mathbb{Z}$.

```
EV=FreeModule(ZZ,3)
w=EV([1,1,-4])
A=EM([1,2,3,3,2,1,1,1,1])
A,w
V=EM(1)
V
V[0,1]=2
V
```

Exercice 4 – [Relation de Bézout et calcul matriciel]

1) Soient deux entiers a et b tels que $(a, b) \neq (0, 0)$. Soient u et v deux entiers tels que $au + bv = \text{pgcd}(a, b)$. Déterminer en fonction de a, b, u, v et $d = \text{pgcd}(a, b)$ une matrice $U \in \mathcal{M}_2(\mathbb{Z})$ de déterminant 1 telle que $(a, b)U = (\text{pgcd}(a, b), 0)$.

2) En s'inspirant de la question précédente, montrer qu'il existe une matrice U dans $\mathcal{M}_n(\mathbb{Z})$ de déterminant 1) telle que

$$(a_1, \ldots, a_n)U = (\text{pgcd}(a_1, \ldots, a_n), 0, \ldots, 0)$$

et programmer le calcul de cette matrice.

Pour cela, on peut d'abord calculer une matrice V_1 telle que

$$(a_1, \ldots, a_n)V_1 = (\text{pgcd}(a_1, a_2), 0, a_3, \ldots, a_n),$$

puis une matrice V_2 telle que

$$(\text{pgcd}(a_1, a_2), 0, a_3, \ldots, a_n)V_2 = (\text{pgcd}(a_1, a_2, a_3), 0, 0, a_4, \ldots, a_n)$$

et itérer le processus. Alors la matrice U cherchée est égale au produit des V_i.

3) Si $b \in \mathbb{Z}$ et $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ sont fixés, expliquer (sans le programmer) comment résoudre l'équation $\sum a_i x_i = b$ en nombres entiers (x_i) [*intercaler* $UU^{-1} =$ Id]. Résoudre les équations $1009x + 345y + 56z = 1$ et $143x + 195y + 165z = 3$.

4) Comment résoudre un système de plusieurs équations sur $\mathbb{Z}^n$? Il n'est pas demandé de programmer ce calcul.

Exercice 5 – [Restes Chinois]

En utilisant la commande `crt`, résoudre les systèmes

$$\begin{cases} x \equiv -1 \mod 21 \\ x \equiv 11 \mod 25 \\ x \equiv 1 \mod 16 \end{cases}, \quad \begin{cases} x \equiv -1 \mod 21 \\ x \equiv 11 \mod 15 \\ x \equiv 1 \mod 10 \end{cases} \text{ et } \begin{cases} x \equiv -1 \mod 21 \\ x \equiv 10 \mod 15 \\ x \equiv 1 \mod 10 \end{cases}$$

Note. Cette commande `crt` s'applique à tout anneau euclidien par exemple à $k[x]$, où k est un corps.

Note. On connaît bien l'algorithme correspondant dans le cas où les moduli sont deux à deux premiers entre eux. Il ne s'applique tel qu'à l'un de ces trois exemples. L'exercice 4 de la feuille 6 montre comment on peut adapter l'algorithme au cas de moduli non deux à deux premiers entre eux.