L3 Alg effective TD-TP2

26 sept. 2016

Calcul du pgcd et d'une relation de bezout

Ex. Soient $a_1, \dots, a_n, d$ des entiers. Montrer que si $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$ alors d divise $a_1, \dots, a_n$ et d est combinaison linéaire à coefficients entiers de $a_1, \dots, a_n$ (relation de Bezout).
Inversement si l'entier e divise $a_1, \dots, a_n$ alors $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} \subset e\mathbb{Z}$
En déduire qu'on a $a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$ si et seulement si d est le plus grand diviseur commun de $a_1, \dots, a_n$.

Ex Soient a, b, c trois entiers avec $b \neq 0$. Prouver que a divise bc si et seulement si le quotient a/pgcd(a,b) divise c. (Utiliser une relation de Bezout.) Que se passe t-il si $b = 0$?

Ex 1.a. La fonction suivante prend deux entiers et rend une suite d'entier. Sa définition est elle récursive ou itérative ? Que calcule la fonction ? Essayer avec (132,105)

```
def rel (a,b):
    if b==0:return(a,1,0,1)
    else:
        d,u,v,c=rel(b,a%b)
        #print(d,u,v)
        return(d,v,u-v*(a//b),c+1)
```

1.b. Listes d'éléments dans Sage. Expérimenter les instructions suivantes ; Voir aussi la feuille de référence Sage - Algèbre au dos de la feuille de TD1

```
l=[1,2,1];l,type(l),len(l)
l[0],l[len(l)-1] # l'indice commence à 0 et s'arrête à len(l)-1
```

```
([1, 2, 1], <type 'list'>, 3)
(1, 1)
```

```
l=l+[2,2];l
l[0:3]
l[3:0]
[2*l[i-1] for i in [1..len(l)]]
```

1.c. On suppose donné un algorithme de calcul du pgcd de deux entiers et d'une relation de Bezout associée (xgcd(a,b)dans Sage par exemple). Observer qu'on a

$$a_1\mathbb{Z} + \cdots + a_n\mathbb{Z} \;=\; a_1\mathbb{Z} + \cdots + a_{n-2}\mathbb{Z} + \left(a_{n-1}\mathbb{Z} + a_n\mathbb{Z}\right)$$

En déduire une relation entre $\mathrm{pgcd}(a_1, \dots, a_n)$, $a_1,,a_{n-2}$ et $\mathrm{pgcd}(a_{n-1}, a_n)$ puis un algorithme récursif de calcul du pgcd de n entiers. Construire de même une relation de Bezout associée au pgcd de n entiers.

1.d. La fonction suivante utilise la fonction rel ci-dessus ; il faut donc que Sage connaisse rel avant l'execution des instruction ci-dessous. Que calcule cette fonction ? Expliquer

```
def rell (l):
    n=len(l)
    if n==1:return(l[0],[1])
    else:
```

```
        a,b=rell(l[0:n-1])
        d,u,v,c=rel(a,l[n-1])
        return(d,[u*b[i] for i in [0..n-2]]+[v])
```

```
rell([105,132,5])
```
```
(1, [-10, 8, -1])
```

Equations linéaires sur $\mathbb{Z}$

Ex.a. Soient $a_1, \dots, a_n, b$ des entiers. Montrer que l'équation $a_1x_1 + \cdots + a_nx_n = b$ admet une solution entière si et seulement si le pgcd de $a_1, \dots, a_n$ divise b.
Dans le cas $b = \text{pgcd}(a_1, \dots, a_n)$, pouvez vous expliciter une solution ? Pouvez vous expliciter une solution dans le cas général ?

Ex.b. Soit x un entier fixé. Montrer que l'équation $a_1x_1 + \cdots + a_{n-1}x_{n-1} + a_nx = 0$ admet une solution entière si et seulement si x est multiple d'un certain entier x' à déterminer. Pouvez vous exhiber une solution particulière $x'_0, \dots, x'_{n-1}$ dans le cas $x = x'$?
Montrer que toute solution de l'équation homogène $\sum a_ix_i = 0$ s'écrit de manière unique comme somme d'une solution de la forme $(x_1, \dots, x_{n-1}, 0)$ et d'un multiple de la solution particulière $(x'_0, \dots, x'_{n-1}, x')$.
En déduire un algorithme récursif de calcul d'une base sur $\mathbb{Z}$ des solutions de l'équation homogène.

Méthodes matricielles
Voir la feuille de référence Sage - algèbre linéaire.
On ne peut pas multiplier une matrice avec une liste ; il faut d'abord convertir la liste en vecteur. Ex :

```
A=matrix(ZZ,[[1,2],[0,1]]);A
```
```
[1 2]
[0 1]
```

```
l=[1,0];x=vector(l);x
```
```
(1, 0)
```

```
A*x;x*A
```

A quelle condition sur a, b, c, d la matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

est elle inversible dans $\text{M}_2(\mathbb{Z})$?

Ex. Soient a, b deux entiers non tous nuls et soit d leur pgcd.
Trouver une matrice M inversible dans $\text{M}_2(\mathbb{Z})$ telle qu'on ait $(a, b) * M = (d, 0)$. Trouver de même une matrice N telle qu'on ait $N * (a, b) = (d, 0)$.

Ex. Soit $A \in \text{M}_2(\mathbb{Z})$ une matrice. Montrer qu'on peut transformer A par multiplication à gauche et à droite par des matrices inversibles en une matrice diagonale où le premier élément de la diagonale divise le second. Algorithme ?