UNIVERSITÉ MONTPELLIER 2
SCIENCES ET TECHNIQUES

FLMA607 – Calcul formel – 2010-2011

TP 2 : Un algorithme modulaire

Exercice 1

1) Effectuer un pivot de Gauss sur la matrice $A_\lambda = \begin{pmatrix} 1 & -1 & 1 \\ 5 & 2 & -1 \\ 3 & 4 & \lambda \end{pmatrix}$

- sans maple
- manuellement en utilisant la commande `RowOperation` de maple (consuler l'aide).

```
> A:=Matrix(3,3,[[1,-1,1],[5,2,-1],[3,4,lambda]]);
> A0:=A;
> A0:=RowOperation(A0,[2,1],-5);
```

⋮

- directement à l'aide de la commande `GaussianElimination` de maple.

2) Quel est le rang de cette matrice ? Que répond Maple à cette question ? Conclusion.

Exercice 2

Soient les matrices $A = \begin{pmatrix} 1 & 0 & 10 & 5 \\ 3 & 1 & -4 & -1 \\ 4 & 1 & 6 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & -2 & -1 & 3 & 1 \\ 2 & -4 & 1 & 0 & 5 \\ 1 & -2 & 2 & -3 & 4 \end{pmatrix}$. À l'aide de la commande maple `RowOperation`, effectuer un pivot de Gauss sur les matrices A et B. Vérifier les résultats à l'aide de la commande `GaussianElimination`.

Exercice 3

On désire calculer le déterminant d'une matrice carrée $A = (a_{ij})_{i,j\in\{1,\dots,n\}} \in M_n(\mathbb{Z})$.

1) Quel est le coût de l'algorithme reposant sur la formule $\det A = \sum_{\sigma\in\mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i\sigma(i)}$?

2) On peut aussi calculer le déterminant d'une matrice à coefficients dans $\mathbb{Z}$ par la méthode du pivot de Gauss dans $\mathbb{Q}$. Montrer que le nombre d'opérations effectuées dans $\mathbb{Q}$ est alors polynomial en n.

3) À l'aide de la commande maple `RowOperation`, calculer « à la main » le déterminant de la matrice $A = \begin{pmatrix} 6 & -2 & 11 & -17 & 18 \\ -13 & 20 & -28 & -16 & -23 \\ -19 & 15 & 18 & 13 & -14 \\ 23 & 23 & 12 & 6 & 0 \\ 2 & 3 & 6 & 24 & -10 \end{pmatrix}$. Que constatez-vous quant à la taille des coefficients des matrices intermédiaires [1] ?

Dans la suite de cette exercice, on propose une autre approche pour calculer le déterminant d'une matrice à coefficients entiers, avec laquelle on évite cette « explosion des coefficients ».

4) Écrire une procédure `detmodp` qui prend en entrée une matrice carrée A à coefficients entiers et un nombre premier p, et qui rend en sortie $\det A \mod p$. Le calcul sera fait par l'algorithme du pivot de Gauss, que l'on implémentera entièrement. On pourra utiliser `SwapRow` pour échanger deux lignes. Tous les calculs doivent être faits modulo p pour garantir que la taille des coefficients des calculs intermédiaires reste bornée. Pour calculer l'inverse de la classe d'un entier n dans $\mathbb{Z}/p\mathbb{Z}$ il suffit de faire `1/n mod p;` .

5) On admettra ici que le déterminant d'une matrice $A = (a_{ij}) \in M_n(\mathbb{Z})$ est majoré par la borne de Hadamard

$$|\det A| \leq H = n^{n/2}(\max_{1\leq i,j\leq n} |a_{ij}|)^n.$$

Écrire une procédure `borne_hadamard` qui prend en entrée une matrice $A \in M_n(\mathbb{Z})$ et qui calcule cette borne.

1. On pourrait donc craindre que ce phénomène ruine la complexité réelle de l'algorithme, c'est-à-dire le nombre d'opérations sur des mots-machines effectuées. En fait, le coût reste malgré tout polynomial mais la preuve est non triviale.

6) Écrire une procédure `listepremiers` qui prend en entrée un entier H et qui retourne la liste $[p_1, \ldots, p_r]$ des r premiers nombres premiers, où r est le plus petit entier tel que le produit des p_i soit strictement supérieur à $2H$ (`?ithprime`).
7) Écrire une procédure `chinois` qui prend en entrée r entiers $m_1, \ldots, m_r$ deux à deux premiers entre eux et r entiers $d_1, \ldots, d_r$, et qui retourne l'unique entier d tel que

$$-\frac{m}{2} < d \leq \frac{m}{2} \text{ et } \forall i \in \{1, \ldots, r\}\ d \equiv d_i \mod m_i$$

où $m = m_1 \ldots m_r$. On pourra utiliser la procédure maple `chrem` (consulter l'aide).
8) En utilisant les procédures des questions 4)-7), écrire une procédure qui calcule le déterminant d'une matrice carrée à coefficients entiers. Prouver que votre algorithme est correct. Tester sur quelques exemples.