FEUILLE D'EXERCICES n° 7

Théorème de Bézout, restes chinois, calcul modulaire

Exercice 1 – [Autour de Bézout]

1) 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. En utilisant cette commande, écrire un algorithme qui prend en entrée une famille d'entiers $(a_1, \dots, a_n)$ et donne en sortie $(u_1, \dots, u_n) \in \mathbb{Z}^n$ tel que

$$\sum_{i=1}^{n} a_i u_i = \mathrm{pgcd}(a_1, \dots, a_n).$$

2) Interpréter l'algorithme d'Euclide étendu comme une suite de modification du système linéaire d'inconnues (a, b)

$$\begin{pmatrix} u_x & v_x \\ u_y & v_y \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix}.$$

3) Trouver une matrice U de déterminant ± 1 telle que $(a, b)U = (\mathrm{pgcd}(a, b), 0)$.

4) En s'inspirant de la question précédente, montrer qu'il existe une matrice U dans $\mathrm{GL}(n, \mathbb{Z})$ (entière, de déterminant ± 1) telle que

$$(a_1, \dots, a_n)U = (\mathrm{pgcd}(a_1, \dots, a_n), 0, \dots, 0),$$

et programmer le calcul de cette matrice. [*ne traiter que 2 coordonnées à la fois*]

Note. Cette question est une version "concrète" (d'un cas particulier) du théorème des diviseurs élémentaires pour les modules de type fini sur les anneaux principaux [*appliqué au dual* $(\mathbb{Z}^n)^*$ *et au sous* $\mathbb{Z}$*-module engendré par la forme linéaire* $(a_1, \dots, a_n)$]. Les diviseurs élémentaires sont donnés par le membre de droite.

Programmer le calcul de U [*se rappeler l'astuce de la matrice identité auxiliaire dans l'algorithme du pivot de Gauss*]. Que dire de sa première colonne ? Si b et $(a_1, \dots, a_n)$ sont des entiers fixés, expliquer comment résoudre l'équation $\sum a_i x_i = b$ en nombre entiers (x_i) [*intercaler* $UU^{-1} = \mathrm{Id}$]. Résoudre les équations $1009x + 345y + 56z = 1$ et $143x + 195y + 165z = 3$.

5) Comment résoudre un système de plusieurs équations sur $\mathbb{Z}^n$? [*la question précédente permet de se ramener à un système triangulaire*]

Exercice 2 – [Restes Chinois]

1) Donner un algorithme permettant de décider si un entier x est inversible dans $(\mathbb{Z}/n\mathbb{Z})^*$, et le cas échéant de déterminer son inverse.

2) Résoudre les systèmes

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

(on pourra utiliser la commande `crt`).

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

On connaît bien l'algorithme correspondant dans le cas où les modules sont deux à deux premiers entre eux. Il ne s'applique pas tel quel aux exemples précédents. Les questions suivantes portent sur le cas général.

3) Soient a et b deux entiers > 0. On considère le système d'inconnue N

$$\begin{cases} N & \equiv & \alpha \pmod{a} \\ N & \equiv & \beta \pmod{b} \end{cases}$$

et on pose $\delta = \text{pgcd}(a, b)$, puis u et v deux entiers tels que $au + bv = \delta$.

a) Montrer que le système n'a pas de solution si $\alpha \not\equiv \beta \pmod{\delta}$.

b) Sinon, montrer que

$$N := \alpha + u\frac{a}{\delta}(\beta - \alpha) = \beta + v\frac{b}{\delta}(\alpha - \beta) = u\frac{a}{\delta}\beta + v\frac{b}{\delta}\alpha$$

convient. Montrer que cette solution est unique modulo ab/δ.

Note. c'est une généralisation du "théorème chinois" au cas ou les modules ne sont pas nécessairement premiers entre eux. Si $\delta = \text{pgcd}(a, b) = 1$, on trouve bien un isomorphisme (explicite) entre $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$ (qui à (α, β) associe N).

4) En déduire un algorithme pour résoudre un nombre quelconque de congruences simultanées, et le programmer. Il s'agit là d'un exercice. Pour ce calcul, il faudra ensuite utiliser la commande `crt`.

5) Après une série de rapines, une troupe de 14 pirates partage (équitablement) le butin et laisse le reliquat, 3 écus, au cuisinier chinois, le 15ème homme d'équipage. Le lendemain, un flibustier tombe à la mer et n'est pas repéché à temps ; après avoir envisagé le versement de sa part à des œuvres, les pirates refont le partage en incluant sa part ; le cuistot reçoit 2 écus. La semaine se passe sans encombres, mais trois pirates ivres se disputent sur leurs parts respectives et deux d'entre eux sont tués. Notre cuisinier récupère 5 écus. La fin du mois est mauvaise et 3 pirates périssent dans une embuscade ; mais le cuistot est content : il garde ses 5 écus.

Quel magot peut-il espérer empocher quand il décide d'empoisonner le reste de la bande ?

Exercice 3 – [Déterminant modulaire]

Soit $A \in M_n(\mathbb{Z})$. On se propose de calculer $\det A$ de façon modulaire, c'est-à-dire de calculer $\det A \pmod{p}$ à partir des $a_{i,j} \pmod{p}$, pour des p premiers et petits, et d'en déduire la valeur de $\det A$. Pour cela il faudra prendre des p dont le produit est plus grand que $2|\det A|$ et se servir du lemme chinois. On rappelle l'inégalité de Hadamard :

$$|\det A|^2 \leqslant \prod_{j=1}^{n} \Big(\sum_{i=1}^{n} a_{i,j}^2 \Big),$$

qui aidera à déterminer une famille de p adaptée.

1) Écrire une procédure admettant en entrée A et qui détermine successivement une famille appropriée de premiers, les déterminants modulaires puis le déterminant de A. Faire attention aux fonctions `mod`$(*, d)$ ou $*\%d$ qui renvoient un entier de l'intervalle $[0, d[$ et non de $]-\frac{d}{2}, \frac{d}{2}]$.

2) Tester sur $A \in M_{10}(\mathbb{Z})$ où les $a_{i,j}$ sont aléatoires et vérifient $|a_{i,j}| < 100$. Étendre les tests.