Préparation à l'agrégation *Année 2018/2019*

université PARIS DIDEROT PARIS 7

MODÉLISATION — ALGÈBRE ET CALCUL FORMEL

Pgcd, algorithme d'Euclide et variantes

A. CHAMBERT-LOIR

L'anneau $\mathbf{Z}$ des entiers et l'anneau $k[T]$ des polynômes en une variable à coefficients dans un corps k disposent d'une *division euclidienne* tel que le reste soit strictement « plus petit » que le diviseur, mesuré par une fonction φ à valeurs dans $\mathbf{N}$ (*stathme*), respectivement donnée par $\varphi(a) = |a|$ et $\varphi(a) = \deg(a)$.
L'axiome essentiel est le suivant : pour tous a, b, avec $b \neq 0$, il existe q, r tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$; on ajoute parfois la condition $\varphi(ab) \geqslant \varphi(a)$ pour tous a, b.

1 Explorer le logiciel de calcul formel et apprendre à réaliser des divisions euclidiennes dans ces deux cas. Calculer par exemple le pgcd de 123 et 234, ou de $3T^4 - 6T^3 + 13T^2 - 8T + 12$ et $6T^5 + 17T^3 - 3T^2 + 12T - 4$.

2 D'autres anneaux possèdent une division euclidienne. On explorera ici le cas des anneaux $A = \mathbf{Z}[i]$ et $A = \mathbf{Z}[\sqrt{2}]$, munis des stathmes définis par $\varphi(a+bi) = |a+bi|^2 = a^2 + b^2$ et $\varphi(a + b\sqrt{2}) = \left|a^2 - 2b^2\right|$.

a) Programmer les opérations arithmétiques de base dans ces anneaux (addition, soustraction, multiplication) et dans leurs corps des fractions $F = \mathbf{Q}[i]$ et $F = \mathbf{Q}[\sqrt{2}]$ (division).

b) Démontrer que ces anneaux possèdent une division euclidienne, définie comme suit pour $A = \mathbf{Z}[i]$: calculer le quotient $a/b = u + vi$ dans $\mathbf{Q}[i]$; noter u' et v' les entiers les plus proches de u et v, puis $q = u' + v'i$ et $r = a - bq$.

c) Programmer ces divisions euclidiennes.

3 Un anneau euclidien étant factoriel, et même principal, tout couple (a, b) d'éléments d'un tel anneau possède un « plus grand diviseur commun » d :

cet élément d divise a et b, et tout élément qui divise a et b divise également d. On écrira par abus $d = \mathrm{pgcd}(a,b)$; par abus, car tout élément de la forme ud, où u est inversible, est encore un plus grand diviseur commun. En fait, cet élément est un générateur de l'idéal (a,b) engendré par a et b.
L'*algorithme d'Euclide* le calcule ainsi : on construit une suite $(a_1, a_2, \ldots)$, éventuellement finie, en posant $a_1 = a$, $a_2 = b$, puis, si a_n est défini et non nul, avec $n \geqslant 2$, on choisit une division euclidienne $a_{n-1} = a_n q + r$, et on pose $a_{n+1} = r$. Comme la suite $(\varphi(a_n))_{n\geqslant 2}$ est une suite strictement décroissante d'entiers $\geqslant 0$, la suite (a_n) est finie. Il existe $n \geqslant 2$ tel que $a_n = 0$, et a_{n-1} est un plus grand diviseur commun de a et b.

a) Explorer les routines du logiciel permettant de calculer un pgcd dans les deux cas de base $A = \mathbf{Z}$ et $A = k[T]$.

b) Programmer cet algorithme dans ces deux cas.

c) Dans le cas $A = k[T]$, démontrer que l'algorithme se termine au bout d'au plus $\deg(b)$ étapes. Combien de multiplications dans le corps k requiert-il au plus ?

d) Dans le cas $A = \mathbf{Z}$, vérifier que $|a_{n+1}| \leqslant \frac{1}{2}|a_{n-1}|$ pour tout $n \geqslant 2$. En déduire que l'algorithme se termine au bout d'au plus $\lceil \log_2 \max(|a|, |b|) \rceil$ étapes.

4 Puisque le pgcd d de deux éléments a et b engendre l'idéal (a,b), il existe u et v tels que $d = au + bv$ (*relation de Bézout*). L'*algorithme d'Euclide étendu* calcule un tel triplet (d,u,v), de la façon suivante. On pose $(a_1, u_1, v_1) = (a, 1, 0)$, $(a_2, u_2, v_2) = (b, 0, 1)$, puis, si $n \geqslant 2$ est tel que $a_n \neq 0$, on choisit une division euclidienne $a_{n-1} = a_n q + r$ et on pose

$$(a_{n+1}, u_{n+1}, v_{n+1}) = (a_{n-1}, u_{n-1}, v_{n-1}) - q(a_n, u_n, v_n).$$

a) Explorer les routines du logiciel permettant de calculer une relation de Bézout dans les deux cas de base.

b) Programmer l'algorithme d'Euclide étendu dans les deux cas de base, puis dans les deux cas de la question 2.

5 Soit A un anneau euclidien (on pourra se limiter au cas $A = \mathbf{Z}$; le cas d'un corps est également intéressant) et soit $(a_1, \dots, a_n)$ une famille d'éléments de A (non identiquement nulle). Soit M l'ensemble des $(u_1, \dots, u_n) \in A^n$ tels que $u_1 a_1 + \cdots + u_n a_n = 0$.

a) Démontrer que M est un sous-module de A^n (sous-groupe, stable par multiplication par un élément de A ; si $A = \mathbf{Z}$, il s'agit donc juste d'un sous-groupe ; si A est un corps, il s'agit juste d'un sous-espace vectoriel).

b) On part de la matrice

$$\begin{pmatrix} a_1 & 1 & 0 & \dots & 0 \\ a_2 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ a_n & 0 & \dots & 0 & 1 \end{pmatrix}$$

On effectue successivement des opérations sur les lignes ($L_i \to L_i - qL_j$, où $a_i = qa_j + r$ est une division euclidienne, et a_j est un élément de la première colonne où le stathme est minimal). Justifier qu'au bout d'un nombre fini d'opérations, la première colonne contient exactement un coefficient non nul, égal au pgcd de $(a_1, \dots, a_n)$.

c) Utiliser la matrice obtenue pour définir une *base* du sous-module M : des vecteurs $m_1, \dots, m_{n-1} \in M$ tels que tout élément de M s'écrit de façon unique $v_1 m_1 + \cdots + v_{n-1} m_{n-1}$, pour $v_1, \dots, v_{n-1} \in A$.

d) Si $\operatorname{pgcd}(a_1, \dots, a_n) = 1$, utiliser la matrice obtenue pour construire une matrice $P \in \mathrm{SL}(n, A)$ de première colonne $(a_1, \dots, a_n)$.

6 Si a et b sont des éléments d'un anneau euclidien A, il existe plusieurs relations de Bézout $d = au + bv$. Du point de vue de la complexité, il est important de contrôler la taille du résultat. On suppose ici $A = \mathbf{Z}$.

a) Démontrer qu'il existe un couple (u, v) tel que $d = au + bv$,

$$|u| \leqslant \frac{1}{2}|b| \quad \text{et} \quad |v| \leqslant \frac{d}{|b|} + \frac{1}{2}|a|.$$

b) Si $a > b \geqslant 2$, en déduire qu'il existe un couple (u, v) tel que $d = au + bv$ et $|uv| \leqslant (a-1)(b-1)$.

7 D'après le « théorème chinois », si a et b sont des éléments premiers entre eux d'un anneau euclidien, et u, v des éléments de A, il existe un élément w tel que la conjonction de congruences $x \equiv u \pmod{a}$ et $x \equiv v \pmod{b}$ soit équivalente à la congruence $x \equiv w \pmod{c}$.

a) Explorer les routines du logiciel permettant de calculer un tel élément.

b) Utiliser l'algorithme d'Euclide étendu pour le déterminer.

c) Généraliser au cas de n congruences simultanées.

8 Soit ξ un nombre réel ; on note $\lfloor \xi \rfloor$ sa partie entière. Si ξ n'est pas entier, on peut poser $a_0 = \lfloor \xi \rfloor$ et écrire $\xi = a_0 + \dfrac{1}{\xi_1}$, où ξ_1 est un nombre réel tel que $\xi_1 > 1$. Ensuite, on recommence avec ξ_1, d'où une expression

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{\xi_n}}}}$$

(développement en fraction continuée). Pour alléger les notations, lorsque $a_0, \ldots, a_n$ sont des nombres réels, nous poserons

$$[a_0, a_1, \ldots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

a) On définit par récurrence des suites (p_n) et (q_n), par les formules

$$p_{n+1} = a_{n+1} p_n + p_{n-1}, \quad q_{n+1} = a_{n+1} q_n + q_{n-1},$$

avec les conventions $p_{-1} = 1$, $q_{-1} = 0$, $p_{-2} = 0$, $q_{-2} = 1$. (La fraction p_n/q_n est appelée la n-ième réduite de ξ.). Démontrer que l'on a

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$$

et

$$[a_0, \ldots, a_n] = \frac{p_n}{q_n}.$$

Prouver aussi l'égalité

$$\xi = [a_0, \ldots, a_n, \xi_n] = \frac{p_n \xi_n + p_{n-1}}{q_n \xi_n + q_{n-1}}.$$

b) Démontrer que si ces suites sont définies jusqu'au rang n, on a

$$\left| \frac{p_n}{q_n} - \xi \right| < \frac{1}{q_n^2}.$$

c) Si ξ est un nombre rationnel, de la forme a/b, comparer son développement en fraction continuée et l'algorithme d'Euclide appliqué au couple (a, b). En particulier, les suites précédentes sont finies.

d) On suppose que ξ n'est pas un nombre rationnel. Démontrer que la suite (a_n) est infinie et que la suite (p_n/q_n) converge vers ξ.

e) Programmer le calcul de ces suites (à un nombre de termes fixé). Expérimenter le comportement des entiers a_n et des approximations p_n/q_n pour des valeurs diverses de ξ : rationnel, $\xi = (1 + \sqrt{5})/2$ (nombre d'or), $\xi = e$ (qu'observez-vous ?), $\xi = \pi$ (donner ses premières réduites), etc.

f) La Terre parcourt une orbite autour du Soleil en 365,2422 jours environ. Calculer le premiers coefficients du développement en fraction continuée de ce nombre. Sur la seconde réduite, justifier le principe d'une année bissextile tous les 4 ans. Utiliser la quatrième réduite pour justifier d'omettre une année bissextile tous les 400 ans.

g) Le principe de la norme des papiers A0, A1,..., est qu'ils sont rectangulaires, et qu'en découpant en deux une feuille de format Ak, on obtient deux feuilles de format A$(k+1)$; par ailleurs, une feuille A0 est de surface 1 m^2. En pratique, leurs tailles sont arrondies au mm le plus proche. En utilisant

les réduites de $\sqrt{2}$, expliquer pourquoi le papier A0 est de taille 841 mm par 1189 mm.

9 Soit $D \geqslant 2$ un entier naturel sans facteur carré. On suppose que ξ de la forme $u + v\sqrt{D}$, où u et v sont des nombres rationnels.

a) (Idéalement) Programmer le calcul du développement en fraction continuée d'un nombre de cette forme, qui n'utilise que des nombres rationnels.

b) Observer expérimentalement que le développement en fraction continuée d'un tel nombre est périodique à partir d'un certain rang. (Éventuellement, le démontrer en observant que les nombres réels ξ_n qui apparaissent sont également de la forme $u_n + v_n\sqrt{D}$, et que les u_n et v_n ont un même dénominateur commun.)

c) On suppose plus précisément que $\xi = \sqrt{D}$. Observer expérimentalement que son développement en fraction continuée vérifie la condition suivante : il existe un entier $m \geqslant 1$ tel que $a_m = 2a_0$, et $a_{m+n} = a_n$ pour $n \geqslant 1$.

d) Lorsque $n = 2k$ est pair, on écrit $\xi_k = (u + \sqrt{D})/v$; vérifier expérimentalement que $u^2 + v^2 = D$. Cela se produit en particulier lorque D est un nombre premier congru à 1 modulo 4.

e) Vérifier expérimentalement que $p_n^2 - Dq_n^2 = \pm 1$ si et seulement si $m \mid n+1$.