Leçon 142 : PGCD et PPCM, algorithmes de calcul. Applications

Cadre : anneaux factoriels, c'est à dire intègres et avec une décomposition en irréductibles unique à l'ordre près.

1. Rapport du jury. — 2017 : *Il est bien clair que le champ d'étude ne peut se limiter au cas de Z; il s'agit de définir et manipuler les notions de PGCD et PPCM dans un anneau factoriel et comme générateurs de sommes/intersections d'idéaux dans un anneau principal. Le candidat devra prendre soin de différencier le cadre théorique des anneaux factoriels ou principaux dans lequel sont définis les objets et dans lequel s'appliquent les énoncés des théorèmes proposés et le cadre euclidien fournissant les algorithmes. Bien sûr, la leçon peut opportunément s'illustrer d'exemples élémentaires d'anneaux euclidiens, comme Z et K[X]. La leçon doit accorder une part substantielle à la présentation d'algorithmes : algorithme d'Euclide, algorithme binaire, algorithme d'Euclide étendu. Dans le cas des polynômes, on étudiera l'évolution de la suite des degrés et des restes. Il est important de savoir évaluer le nombre d'étapes de ces algorithmes dans les pires cas et on pourra faire le lien avec les suites de Fibonacci. La leçon abordera des applications élémentaires : calcul de relations de Bézout, résolutions d'équations diophantiennes linéaires, inversion modulo un entier ou un polynôme, calculs d'inverses dans les corps de ruptures, les corps finis. On peut aussi évoquer le théorème chinois effectif, la résolution d'un système de congruences et faire le lien avec l'interpolation de Lagrange. Pour aller plus loin, on pourra évoquer le rôle de algorithme d'Euclide étendu dans de nombreux algorithmes classique en arithmétique (factorisation d'entiers, de polynômes, etc). Décrire l'approche matricielle de l'algorithme d'Euclide et l'action de SL2(Z) sur Z2 est tout à fait pertinent. On pourra établir l'existence d'un supplémentaire d'une droite dans Z2, ou d'un hyperplan de Zn, la possibilité de compléter un vecteur de Zn en une base. La leçon peut amener à étudier les matrices à coefficients dans un anneau principal ou euclidien, la forme normale d'Hermite et son application à la résolution d'un système d'équations diophantiennes linéaires. Aborder la forme normale de Smith, et son application au théorème de la base adaptée, permet de faire le lien avec la réduction des endomorphismes via le théorème des invariants de similitude. La leçon invite aussi, pour des candidats familiers de ces notions, à décrire le calcul de PGCD dans Z[X] et K[X,Y], avec des applications à l'élimination de variables. On pourra rappeler les relations entre PGCD et résultant et montrer comment obtenir le PGCD en échelonnant la matrice de Sylvester. Sur l'approximation diophantienne, on peut enfin envisager le développement d'un rationnel en fraction continue et l'obtention d'une approximation de Padé-Hermite à l'aide de l'algorithme d'Euclide, la recherche d'une relation de récurrence linéaire dans une suite ou le décodage des codes BCH.*

2. Le cas modèle $\mathbb{Z}$ et les difficultés d'extension. —

1. *Brefs rappels arithmétiques sans référence aux Idéaux.* — :

- Def : Division euclidienne, divisibilité. Nombres premiers, premiers entre eux.
- Rem : Si le résidu est inférieur en valeur absolu mais positif ou négatif, la division euclidienne n'est pas unique.
- Def : Définition arithmétique du pgcd et du ppcm. Algorithme d'Euclide.
- Lem : Euclide - Si p divide $b\dot{c}$, alors p divise l'un ou l'autre.
- The : Gauss - Si a divise $b\dot{c}$ et a est premier avec b, alors a divise c.
- The : Bezout-Bachet
- Pro : Décomposition en facteurs premiers (théorème fondamental de l'arithmétique). Application de la valuation p-adique aux pgcd et ppcm.
- Pro : $pgcd \cdot ppcm = a \cdot b$.

Algorithme d'Euclide - simple et étendu :

- suite décroissante des résidus (r_{k+1}) : l'algorithme s'arrête en un nombre fini de pas ($\min(|\ a\ |, |\ b\ |)$).
- Pro : $PGCD(r_{k+1}, r_k) = PGCD(r_k, r_{k-1})$.
- Cor : $PGCD(a, b)$ est le dernier résidu non nul du processus.
- App : on a comme application simple la réduction à un dénominateur commun.
- Pro : construction parallèle des facteurs de Bezout par matrice
- App : résolution des équations diophantiennes de degré 1.

Difficultés d'extension

- La division euclidienne nécessite un stathme. On prend le degré des polynômes mais nous n'avons pas toujours la division euclidienne sur $A[X]$ (par opposition à $K[X]$). Exc. : si le coefficient dominant est inversible.
- Bezout n'existe pas partout. *Cexe* : X et Y sont premiers entre eux sur $K[X, Y]$
- Non unicité de la décomposition en éléments irréductibles : sur $\mathbb{F}_4, 2(X + 2) = 2X$

3. Recours aux Idéaux - Extension des notions de divisibilité, irréductibilité et primalité. — On se place dans le cadre d'*anneaux intègres*. On obtient les généralisations suivantes des notions apparues sur $\mathbb{Z}$:

- Def : (a divise b) $\iff$ ($b \in (a)$). On a une correspondance entre la relation de divisibilité et l'inclusion entre idéaux.
- Def : a est associé à $b \iff (a) = (b)$.
- Def : $p \notin A^*$ est irréductible si on a $(p = ab \to (a \in A^* or b \in A^*))$, c'est à dire que les seuls éléments divisant p sont les inversibles et les associés.
- Def : Un idéal I est premier ssi A/I est intègre. Si $I = (p)$ alors p est dit premier.

On ne peut pas généraliser les notions de PGCD ni PPCM

1. *PGCD, PPCM pour les anneaux factoriels.* — On se place dans le cadre d'*anneaux factoriels*. Aux extensions des notions vues avant s'ajoutent les notions de PGCD et de PPCM :

- étant donnés deux éléments de A et leur décomposition en facteurs irréductibles $\mu \Pi p_k^{\phi_k}$.
- Def : on obtient un PGCD en retenant pour chaque facteur irréductible présent dans a ou dans b le min des valeurs p-adiques.

- Def : pour un PPCM on procède de manière identique mais en prenant le max des deux exposants (dont un pouvant être nul).
- Rem : la décomposition étant à un multiple inversible près, on a bien défini "un" PGCD et "un" PPCM.
- Pro : les différents PGCD sont associés entre eux. Idem pour les PPCM.

Exemple d'anneaux non-factoriels. Importance de l'unicité. On a les propriétés suivantes :

- Pro : $a\dot{b} = (a \wedge b)(a \vee b)$
- Pro : $\wedge$ et $\vee$ sont associatives et commutatives.
- Pro : la multiplication est distributive par rapport à $\wedge$
- Lem : lemme d'Euclide
- The : théorème de Gauss - Si $a \wedge b$ alors a/b entraîne a/c.
- Pro : si $b \wedge c = 1$ alors $a \wedge (b\dot{c}) = (a \wedge b)(a \wedge c)$

2. *PGCD, PPCM pour les anneaux principaux.* — On se place dans le cadre d'*anneaux principaux*. Aux extensions des notions vues avant s'ajoutent une nouvelle définition de PGCD et de PPCM, ainsi qu'une généralisation du théorème de Bézout-Bachet :

- Def : étant donnés $a_1, \cdots, a_n \in A$, on dira que a est un PGCD de $(a_1, \cdots, a_n)$ si a génère l'idéal somme des idéaux (a_i).
- Pro : On a donc $(a_1) + \cdots + (a_n) = (a)$ et on note $a_1 \wedge \cdots \wedge a_n$.
- Rem : "un" PGCD et non "le"PGCD. Mais le PGCD est unique à l'association près. Tout élément $u\dot{a}$ où u est inversible est encore un PGCD.
- Def : la notion de PPCM est analogue mais pour l'idéal intersection. $PPCM(a_1, \cdots, a_n) = a$ si $(a) = (a_1) \cap (a_n)$
- Def : on note $a_1 \vee \cdots \vee a_n$.
- Rem : un PPCM est unique à l'association près, c'est à dire à la multiplication par un inversible. et ppcm comme inf et sup de (a) et (b) parmi les idéaux principaux.
- Pro : l'ensemble des idéaux est réticulé avec $(a \wedge b)$ et $(a \vee b)$ comme respectivement max et min.

On a les propriétés suivantes :

- Tout anneau principal est factoriel : nous avons donc les propriétés de la section précédente.
- The : théorème de Bézout - Si $a = a_1 \wedge \cdots \wedge a_n$ alors il existe une combinaison linéaire des a_i égale à a.

Exo : Calculer $(X^m - 1) \wedge (X^n - 1)$.

3. *Cas euclidiens.* — On se place dans le cadre d'*anneaux euclidiens*. L'anneau est donc principal et on a les résultats énoncés au chapitre précédent. On dispose ici de plus d'algorithmes pour calculer concrètement les décompositions en irréductibles, le PPCM, le PGCD et les coefficients de Bézout.

Division Euclidienne

- Def : stathme euclidien
- Exe : anneaux des polynômes sur un corps $\mathbb{K}$ (stathme : degré).
- Cexe : anneaux $\mathbb{Z}[X]$
- Pro : la division euclidienne entre deux éléments d'un anneau A demeure à l'intérieur de A et est donc la même dans tout sur-anneau.
- App : Si on considère un corps k et une extension algébrique $k[\alpha]$ de degré ≥ 2, alors le polynôme minimal de α n'a que des racines $\notin k$.

Algorithme d'Euclide : enchaînements de divisions euclidiennes

- L'algorithme d'Euclide appliqué à a, b puis aux résidus nous donne une suite (r_k, q_k) telle que $r_{k_1} = r_k q_k + r_{d+1}$
- Cette suite est stathme-décroissante et donc finie (stationnaire) puisque les stathmes sont des entiers positifs.
- Pro : on a donc $PGCD(r_{k+1}, r_k) = PGCD(r_k, r_{k-1})$.
- Cor : $PGCD(a, b)$ est le dernier résidu non nul du processus. $r_N = PGCD(a, b)$

Algorithme d'Euclide-Bézout ou Euclide étendu

- L'algorithme d'Euclide-Bézout rajoute les cofacteurs (x_k, y_k) tels que $ax_k + by_k = r_k$.
- Pro : On obtient alors les coefficients de Bézout : $ax_N + by_N = PGCD(a, b)$
- On pose $S_1 = I_2$
- $S_k = \begin{pmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{pmatrix}$
- et $S_{k+1} = S_k \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix}$
- Pro : on démontre alors par récurrence que : $(ab)S_k = (r_k r_{k+1})$.
- Rem : $det(S_k) = -(-1)^k$ donc S_k^{-1} est à termes entiers.
- Nous avons en particulier pour le pas N qui clôt l'algorithme : $(ab)S_N = (r_N 0)$

Résolution des équations diophantiennes linéaires $ax + by = c$.

- CNS : $a \wedge b / c$ ie $c = \lambda a \wedge b$.
- L'algorithme d'Euclide-Bézout nous donne notamment les cofacteurs (x_N, y_N) tels que $\lambda(ax_N + by_N) = c$.
- $\begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix} S_n S_n^{-1} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} r_n & 0 \end{pmatrix} = c$
- Si on note u et v tels que $S_k^{-1} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$ on obtient les CNS $\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} c/r_n \\ l \end{pmatrix}$ où $l \in \mathbb{Z}$.

Nombre d'étapes de l'algorithme d'Euclide-Bézout

- Def : On note $N(a, b)$ le nombre N d'étapes de l'algorithme d'Euclide-Bézout appliqué à (a, b).
- Pro : $N(a, b) \leq 1 + \log_2 a$.
- Pro : si F_n est le n-ième nombre de Fibonacci, $N(a, b) \leq N(F_n, F_{n-1})$ et l'égalité ne se présente que pour $a = F_n$ et $b = F_{n-1}$

Lien avec les fractions continues

– L'algorithme d'Euclide-Bézout nous donne (r_k, q_k, x_k, y_k).
– CNS : $\frac{a}{b} = q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \cdots}}$.

4. Applications importantes. —

– Développement : Berlekamp
– Développement : Théorème de Sophie Germain : "Si p et $q = 2p + 1$ sont deux nombres premiers impairs, alors il n'y a pas de solution entière à $a^p + b^p + c^p = 0$ vérifiant xyz non multiple de p."
– Développement : Décomposition des noyaux (endomorphismes semi-simples).
– décomposition en éléments simples des fractions rationnelles.

Th de Liouville ?
CNS diagonalisaton avec polynome séparable x. Action de SL2(Z) sur Z2 x. forme normale de Smith, et son application au théorème de la base adaptée x. système de congruences et faire le lien avec l'interpolation de Lagrange x. Loi de réciprocité quadratique x. développement d'un rationnel en fraction continue et l'obtention d'une approximation de Padé-Hermite x. . Cryptage BCH

.

Sources :

– *Perrin*
– *Wikipedia*
– *Francinou et Gianella, tome 1 Algèbre*

November 22, 2017

Bruno Nitrosso, EPP et indépendant