142

PGCD et PPCM, algorithmes de calculs. Applications

Cadre : Soit A un anneau commutatif intègre unitaire.

I] PGCD et PPCM ; cas d'un anneau factoriel

A] Définitions et premières propriétés

[1] Def 1 : Soient $a_1,\dots,a_r \in A^*$. On dit que ces éléments admettent un plus grand commun diviseur (PGCD) si $\exists \delta \in A^* / \begin{cases} \forall i \in [\![1;r]\!], \delta \mid a_i \\ \forall a \in A^*, [a \mid a_i\ \forall i \in [\![1;r]\!]] \Rightarrow a \mid \delta \end{cases}$

Ex 2 : 2 est un PGCD de 6 et 8 dans $\mathbb{Z}$ (-2 en est un autre).

[1] Prop-def 3 : Deux PGCD d'une famille finie d'éléments de A^* sont associés. On note dans ce cas $PGCD(a_1,\dots,a_r)$ ou $a_1 \wedge \dots \wedge a_r$ le PGCD de $a_1,\dots,a_r$ modulo les inversibles.

Rem 4 : Si $a \in A^*$ et $b \in A^\times$ alors $PGCD(a,b) = 1$.

Def 5 : $a_1,\dots,a_r \in A^*$ sont dits premiers entre eux (dans leur ensemble) si $PGCD(a_1,\dots,a_r) = 1$. Autrement dits, leurs seuls diviseurs communs sont les inversibles.

Thm 6 : Soient $a_1,\dots,a_r \in A^*$ et $d \in A^*$ et $\alpha_1,\dots,\alpha_r \in A^*$ tels que $\forall i \in [\![1;r]\!], a_i = d\alpha_i$. Alors

$$d = PGCD(a_1,\dots,a_r) \iff PGCD(\alpha_1,\dots,\alpha_r) = 1$$

Def 7 : Soient $a_1,\dots,a_r \in A^*$. On dit que ces éléments admettent un plus petit commun multiple (PPCM) si $\exists \mu \in A^* / \begin{cases} \forall i \in [\![1;r]\!], a_i \mid \mu \\ \forall a \in A^*, [a_i \mid a\ \forall i \in [\![1;r]\!]] \Rightarrow \mu \mid a \end{cases}$

Ex 8 : 24 est un PPCM de 6 et 8. (-24) en est un autre.

[1] Prop-def 9 : Deux PPCM d'une famille finie de A^* sont associés. On note alors $PPCM(a_1,\dots,a_r)$ ou $a_1 \vee \dots \vee a_r$ le PPCM modulo les inversibles.

[1] Thm 10 : Soient $a, b \in A^*$ admettant un PGCD et un PPCM. Alors $ab = PGCD(a,b) \times PPCM(a,b)$

Prop 11 : PGCD et PPCM sont commutatifs et associatifs

B] Cas d'un anneau factoriel

On suppose à partir de maintenant que A est factoriel.

[1] Thm 12 : Soient $a = u \prod_{i=1}^{r} p_k^{n_k}$ et $b = v \prod_{i=1}^{r} p_k^{m_k}$ deux éléments non nuls de A dont on a fait la décomposition en produit de facteurs irréductibles (éventuellement $n_k = 0$ ou $m_k = 0$). Alors $PGCD(a,b) = \prod_{k=1}^{r} p_k^{\min(n_k,m_k)}$

$$PPCM(a,b) = \prod_{k=1}^{r} p_k^{\max(n_k,m_k)}$$

Ex 13 : Ceci peut justifier les exemples 2 et 8.

Rem 14 : Ceci se généralise aisément pour un plus grand nombre d'éléments.

Cor 15 : PGCD et PPCM sont homogènes.

C] Contenu d'un polynôme

[2] Def 16 : Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$. On définit le contenu de P par $C(P) = PGCD(a_0,\dots,a_n)$.

Lem 17 : (DEV 1) $\forall P, Q \in A[X], C(PQ) = C(P)C(Q)$

Thm 18 : (Critère d'Eisenstein) Soit $K = Fr(A)$. Soit $p \in A$ irréductible tel que $\forall i \in [\![0;n-1]\!], p \mid a_i$; $p \nmid a_n$; $p^2 \nmid a_0$. Alors P est irréductible dans $K[X]$

App 19 : $\forall n \in \mathbb{N}^*, X^n - 2$ est irréductible dans $\mathbb{Q}[X]$.

Thm 20 : Les irréductibles de $A[X]$ sont exactement :

- les constantes $p \in A$ irréductibles
- les polynômes non constants de contenu 1 irréductibles dans $K[X]$.

Cor 21 : (Théorème de Gauss) $A[X]$ est factoriel.

II) PGCD et PPCM dans un anneau principal

[1]

Rem 22: Un anneau principal étant factoriel, on dispose déjà de toutes les propriétés précédentes.

Thm 23: Soit δ un PGCD de $a_1,\dots,a_r \in A^*$. Alors $(a_1,\dots,a_r)=(\delta)$. En particulier, $\exists u_1,\dots,u_r \in A$ / $\delta = \sum_{k=1}^{r} u_k a_k$ (relations de Bézout)

Rem 24: Ce résultat ne tient plus dans un anneau factoriel non principal comme $\mathbb{Z}[X,Y]$.

Thm 25: (de Bézout) Soient $a_1,\dots,a_r \in A$ non tous nuls. Alors $PGCD(a_1,\dots,a_r)=1 \iff \exists u_1,\dots,u_r \in A, \sum_{k=1}^{r} u_k a_k = 1$.

Cor 26: (Lemme de Gauss) Soient $a,b,c \in A^*$ avec $a \wedge b = 1$. Si $a \mid bc$ alors $a \mid c$.

Thm 27: Soit μ un PPCM de $a_1,\dots,a_r \in A^*$. Alors $\bigcap_{i=1}^{r} (a_i) = (\mu)$.

Rem 28: Ce résultat reste vrai si A est juste factoriel.

Cor 29: Si $a_1,\dots,a_r \in A$ sont 2 à 2 premiers entre eux alors $PPCM(a_1,\dots,a_r) = \prod_{i=1}^{r} a_i$.

Thm 30: (d'isomorphisme chinois) Soient $a_1,\dots,a_r \in A^*$ 2 à 2 premiers entre eux et $\mu = \prod_{i=1}^{r} a_i$.
Alors $\frac{A}{(\mu)} \simeq \prod_{i=1}^{r} \frac{A}{(a_i)}$

[3]

App 31: (DEV2) [Algorithme de Berlekamp] Soit $q=p^n$ avec p premier et $P=\prod_{i=1}^{r} P_i$ où $P_i \in \mathbb{F}_p[X]$ est irréductible avec $P_i \wedge P_j = 1$ dès que $i \neq j$. Alors il existe $V \in \mathbb{F}_p[X]$ non constant modulo P tel que $P = \prod_{\alpha \in \mathbb{F}_q} PGCD(P, V-\alpha)$

Rem 32: Ceci donne alors un algorithme pour trouver la décomposition en produit de facteurs irréductibles de P

III) Algorithmes de calcul dans un anneau euclidien

On suppose maintenant A euclidien, de stathme φ. Un anneau euclidien étant factoriel, on dispose

A] Recherche du PGCD

[1]

Lem 33: Soient $a,b \in A^*$ et r un reste dans la division euclidienne de a par b. Alors
$$a \wedge b = \begin{cases} b & \text{si } r=0 \\ b \wedge r & \text{sinon} \end{cases}$$

Rem 34: Si $r=0$, le calcul est terminé. Sinon, on a $\varphi(r) < \varphi(b)$ et φ est à valeurs dans $\mathbb{N}$. Donc on peut itérer le processus, qui va alors se terminer. On obtient alors:

Alg 35: (Algorithme d'Euclide) Soient $a,b \in A^*$ tels que $\varphi(b) \leq \varphi(a)$. Soient $q=b$ et r un reste dans la division de a par b. Tant que $r \neq 0$, r devient un reste dans la division de q par r, et q devient le reste précédent. Le processus se termine, et le dernier reste non nul est $a \wedge b$.

[2]

Ex 36: Calculons $111 \wedge 47$: $111 = 47 \times 2 + 17$; $47 = 17 \times 2 + 13$; $17 = 13 \times 1 + 4$; $13 = 4 \times 3 + 1$; $4 = 4 \times 1 + 0$ d'où $111 \wedge 47 = 1$.

[1]

Rem 37: En utilisant l'associativité du PGCD, cet algorithme se généralise pour calculer $PGCD(a_1,\dots,a_r)$, $r \geq 2$.

B] Relations de Bézout

[1]

Alg 38: En écrivant toutes les divisions euclidiennes de l'algorithme d'Euclide, on peut retrouver, en exprimant chacun des restes, les relations de Bézout

[4]

Ex 39: $1 = 13 - 4 \times 3 = 13 - (17 - 13 \times 1) \times 3$

[4] $= 4\times 13 - 3\times 77 = 4\times(47-17\times 2) - 3\times 77$ donne alors $26\times 47 - 11\times 111 = 1$.

[1] Rem 40 : De même, cet algorithme se généralise grâce à l'associativité du PGCD.

IV) Application dans la résolution d'équations en arithmétique.

A] Équations diophantiennes

[2] Def 41 : On appelle équation diophantienne toute équation d'inconnue $x\in\mathbb{Z}$ de la forme $ax\equiv b\,[n]$ où $n\geq 2$, $a\in\mathbb{N}^*$, $b\in\mathbb{Z}$.

Rem 42 : Certaines équations diophantiennes n'admettent pas de solution, par exemple $2x\equiv 1\,[4]$.

[7] Thm 43 : L'équation diophantienne $ax\equiv b\,[n]$ admet une solution si et seulement si $a\wedge n \mid b$. Dans ce cas, si on pose a' et n' tels que $a=(a\wedge n)a'$ et $n=(a\wedge n)n'$ et si on prends $x_0'\in\mathbb{Z}$ tel que $a'x_0'\equiv 1\,[n']$, l'ensemble des solutions est $\{b'x_0'+kn' \mid k\in\mathbb{Z}\}$ où $b=(a\wedge n)b'$.

Rem 44 : La solution particulière peut se trouver grâce à l'algorithme donnant les relations de Bézout.

Ex 45 : On a vu à l'exemple 39 que 26 est solution particulière de $47x\equiv 1\,[111]$. Donc l'ensemble des solutions de $47x\equiv 5$ est $\{130+111k \mid k\in\mathbb{Z}\}$.

Rem 46 : La résolution de ces équations permet par exemple d'inverser, si c'est possible, des éléments de $\mathbb{Z}/n\mathbb{Z}$.

Ex 47 : $\overline{47}$ est inversible dans $\mathbb{Z}/111\mathbb{Z}$ et son inverse est $\overline{26}$.

B] Système diophantien

On souhaite, étant donnés $n_1,\dots,n_r$ 2 à 2 premiers entre eux, résoudre : $\forall i\in[\![1;r]\!]$, $x\equiv a_i\,[n_i]$ où $a_i\in\mathbb{Z}$ $\forall i\in[\![1;r]\!]$.
Le théorème d'isomorphisme chinois donne une façon de résoudre ce système :

Thm 48 : Soient $\mu=\prod_{i=1}^{r} n_i$ et $m_i=\frac{\mu}{n_i}$ $\forall i\in[\![1;r]\!]$. Par Bézout, $\exists u_1,\dots,u_r\in\mathbb{Z}$, $\sum_{i=1}^{r} u_i m_i = 1$. Alors [7]

$$\Psi : \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z} \longrightarrow \mathbb{Z}/\mu\mathbb{Z}, \quad (\overline{x_1},\dots,\overline{x_r}) \longmapsto \overline{\sum_{i=1}^{r} u_i m_i x_i}$$

est un isomorphisme.

Cor 49 : L'ensemble des solutions du système est $\{x_0+k\mu \mid k\in\mathbb{Z}\}$ où x_0 est solution particulière.

Ex 50 : On souhaite résoudre $\begin{cases} x\equiv 5\,[47] \\ x\equiv 3\,[111] \end{cases}$
Alors une solution particulière possible est $x_0 = 26\times 47\times 3 - 11\times 111\times 5$.

Références:

- Algèbre et géométrie, Rombaldi [1]
- Cours d'algèbre, Perrin [2]
- Objectif agrégation, Beck [3]
- Algèbre, Gourdon [4]