142 – PGCD et PPCM, algorithmes de calcul. Applications.

Références : Rombaldi, Gourdon Algèbre, Perrin, *Mathématiques L1 : Cours complet avec 1000 tests et exercices corrigés* Marco.

Cadre : $(A,+,\times)$ un anneau intègre. L'objectif est de généraliser les notions de PGCD et PPCM connus sur $\mathbb{N}$ sur des anneaux.

1 Définition du PGCD et PPCM sur un anneau factoriel

Définition 1. Soit $(a,b) \in A$. On dit que a divise b si il existe $c \in A$ tel que $b = ac$.
On dit que a est irreductible si $a \notin A^\times$ et $a = bc \implies b \in A^\times ouc \in A^\times$.
On dit que a est premier si $a \notin A$ et $a|bc \implies a|b$ ou $a|c$.

Définition 2. Un anneau A est dit factoriel si pour tout $a \in A$ non-inversible, il existe des éléments irreductibles $(p_1,...,p_r)$ de A et un élément inversible u tel que $a = u \times p_1 \times ... \times p_r$. Cette décomposition est unique à l'ordre des facteurs près.

Proposition 3. *Dans un anneau factoriel, p est premiers $\iff$ p est irreductible.*

Exemple 4. $\mathbb{Z}$, $\mathbb{K}[X]$ avec $\mathbb{K}$ un corps sont des anneaux factoriels.

Définition 5. Soit a,b dans A, avec les décompositions $a = u\Pi_{i=1}^r p_i^{n}{}_i$ et $b = v\Pi_{i=1}^r p_i^{m}{}_i$ avec n_i, m_i des entiers éventuellement nul.
On définit le PGCD de deux élément par $a \wedge b = \Pi_{i=1}^r p_i^{\min(n_i,m_i)}$ et le PPCM par $a \vee b = \Pi_{i=1}^r p_i^{\max(n_i,m_i)}$

Remarque 6. Il n'y a pas unicité du PGCD et du PPCD puisqu'ils sont définies à un inversible près.
On définit par reccurence le PGCD et PPCM de n éléments.
Deux éléments sont dits premiers entre eux si $a \wedge b \in A^\times$.

Proposition 7.
— *Si c divise a et b, alors c divise $a \wedge b$*
— *si a et b divise c, alors $a \vee b$ divise c.*

Exemple 8. $6 \wedge 21 = 3$ dans $\mathbb{Z}$.
$X^2 - 1 \wedge X - 1 = X - 1$ dans $\mathbb{R}[X]$
$X^2 - 9 \vee X^2 + 5X + 6 = (X^2 - 9)(X + 2)$ dans $\mathbb{R}[X]$.

Proposition 9. *Soit $(\lambda, a_1, ..., a_n) \in A^*$. Alors $\lambda a_1 \wedge ... \wedge \lambda a_n = \lambda a_1 \wedge ... \wedge a_n$. (De même pour le PPCM).*

Proposition 10. *Pour tout $a, b \in A$, $a \wedge b \times a \vee b = a \times b$ à un inversible près. Donc si a et b sont premiers entre eux, on à $a \vee b = ab$ à un inversible près.*

Définition 11. Soit P $\in A[X]$ (A factoriel), on définit le contenu de P comme étant le PGCD de ses coefficients. On le note c(P).

Lemme 12. *Lemme de Gauss pour les polynômes. $c(PQ) = c(P)c(Q)$*

Théorème 13 (Critère d'irreductibilité d'Eisenstein). *Soit $P = \sum_{k=0}^{n} a_k X^k \in A[X]$ et p un nombre premier. On suppose que $p|a_i \forall i \in \{0,...,n-1\}$, p ne divise pas a_n et p^2 ne divise pas a_0. Alors P est un polynôme irreductible de FracA[X]*

2 Anneaux principeaux et relation de Bézout

Définition 14. Un anneau A est dit principal si tout les idéaux I de A peuvent s'écrire I=(a) avec a un élément de A

Proposition 15. *Si a|b, on à $(b) \subset (a)$.*

Proposition 16. *Un anneau principal est factoriel*

Remarque 17. Il est possible de définir autrement le PGCD et le PPCM sur un anneau principal. Cette nouvelle définition est équivalente à celle donnée précédemment.

Définition 18. Soit A principal. On appelle PGCD de $(a_1,...a_n)$ l'élément qui engendre l'idéal $(a_1) + ... + (a_n)$. On appelle PPCM l'élément qui engendre l'idéal $(a_1) \cap ... \cap (a_n)$

Théorème 19 (Relation de Bézout). *$d = a_1 \wedge ... \wedge a_n \iff$ il existe des éléments $(u_1,...,u_n)$ dans A tel que $d = a_1u_1 + ... + a_nu_n$.*

Application 20 (Lemme des noyaux). *Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $f \in L(E)$. Soit $P = P_1...P_r$ avec $P_i \in \mathbb{K}[X]$ des polynômes premiers entre eux deux à deux. Alors $Ker(P(f)) = \bigoplus_{i=1}^{r} Ker(P_i(f))$.*

Corollaire 21 (Lemme de Gauss). *Si a|bc et a et b sont premiers entre eux, alors a|c.*

Théorème 22 (Des restes chinois). *Soient $(n_1, ..., n_r)$ des éléments de A principal premiers deux à deux entre eux. On pose $n = n_1 \times ... \times n_r$. Alors on à $\frac{\mathbb{A}}{(n)} \simeq_{\varphi} \frac{A}{(n_1)} \times ... \times \frac{A}{(n_r)}$ à l'aide de l'application :*

$$\begin{aligned} \varphi : \quad & \frac{A}{(n)} \to \frac{A}{(n_1)} \times ... \times \frac{A}{(n_r)} \\ & \pi_n(a) \mapsto (\pi_{n_1}(a), ..., \pi_{n_r}(a)) \end{aligned} \tag{1}$$

L'application réciproque est

$$\begin{aligned} \varphi^{-1} : \quad & \frac{A}{(n_1)} \times ... \times \frac{A}{(n_r)} \to \frac{A}{(n)} \\ & (\pi_{n_1}(a_1), ..., \pi_{a_r}(k)) \mapsto \pi_n(\sum_{i=1}^{r} a_i u_i \frac{n}{n_i}) \end{aligned} \tag{2}$$

où les $(u_i) \in A^r$ vérifient : $\sum_{i=1}^{r} u_i \frac{n}{n_i} = 1$

Remarque 23. Ce théorème permet de résoudre des systèmes de congruence dans $\mathbb{Z}$ où $\mathbb{K}[X]$. Mais pour cela, on à besoin d'être capable de calculer des relations de Bézouts ! C'est le but de la prochaine partie.

Théorème 24 (de l'élément primitif). *Soit $\mathbb{K}$ un corps commutatif de caractéristique nulle et $\mathbb{L}$ un surcorps de $\mathbb{K}$. Si $\mathbb{L}$ est un $\mathbb{K}$-e.v de dimension finie, alors il existe $x \in \mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}[x]$*

3 Anneaux euclidiens et algorithmes de calculs

3.1 Algorithme d'Euclide, calcul de PGCD

Définition 25. Un anneau A est dit euclidien si il existe un stahtme φ, une application de $A \mapsto \mathbb{N}$ tel que $\forall (a, b) \in A$, avec $b \neq 0$, il existe un couple $(q, r) \in A^2$ tel que $a = bq + r$ avec $r = 0$ où $\varphi(r) < \varphi(b)$.

Exemple 26. Z est un anneau euclidien avec le stathme valeur absolue.
$\mathbb{K}[X]$ est un anneau euclidien avec le degré pour stathme

Théorème 27. *Un anneau euclidien est principal.*

Lemme 28 (d'Euclide). *On reprend les notations de la définition précédente.*

$$a \wedge b = \begin{cases} b & si\ r = 0 \\ b \wedge r & sinon. \end{cases}$$

Méthode 29 (D'euclide). On donne l'algorithme d'Euclide qui permet de calculer le PGCD de deux éléments. (voir Rombaldi)

Application 30. $157 \wedge 24 = 1$
$424 \wedge 68 = 4$
$5^{n+1} - 1 \wedge 5^n - 1 = 4$
$X^5 - X^4 + X^3 - X^2 + X - 1 \wedge X^2 - 1 = X - 1$
$X^3 + X^2 + X + 1 \wedge X + 1 = X + 1$

3.2 Algorithme d'Euclide étendu

Méthode 31. En remontant l'algorihme d'Euclide, on est capable de déterminer une relation de Bézout.

Exemple 32. $1 = 72 \times 24 - 11 \times 157$

Pour $X - 1$ et $X + 2$ on à : $\frac{X+2}{3} - \frac{X-1}{3} = 1$

Pour $X + 1$ et $X^2 - 2X + 1$ on à : $\frac{X^2 - 2X + 1}{4} - \frac{X-3}{4}(X + 1) = 1$

Théorème 33 (De Bézout). $d = a_1 \wedge ... \wedge a_n \iff$ *Il existe des entiers relatifs $(u_1, ..., u_n)$ tel que $d = a_1 u_1 + ... + a_n u_n$.*

Méthode 34 (Algorithme d'Euclide). On est concrètement capable de construire les entiers $(u_1, ..., u_n)$ précédents grâce à l'algorithme d'Euclide.

Exemple 35. $157 \wedge 24 = 1$ puis $1 = 72 \times 24 - 11 \times 157$

3.3 Application à la résolution d'équation diophantienne

Théorème 36 (Equation diophantienne de degré 2). *On considère l'équation $ax + by = c$, avec a,b et c trois entiers relatifs.*
Cette équation admet des solutions $\iff$ $a \wedge b$ divise c.
Dans ce cas, l'ensemble des solutions est les couples $(x, y) = (x_0, y_0) + \frac{k}{a \wedge b}(b, -a$ avec $k \in \mathbb{Z}$, avec (x_0, y_0) une solution particulière de l'équation (donnée par l'algorithme d'Euclide étendue).

Exemple 37.
— Pour l'équation $3x + 2y = 5$, l'ensemble des solutions est $(5, -5) + k \times (2, -3)$, pour $k \in \mathbb{Z}$.
— L'équation $12x + 8y = 5$ n'admet pas de solutions.

Théorème 38. *On s'intéresse à l'équation de congruence $ax \equiv b \pmod{n}$, avec $n > 1$, a un entier naturel et b un entier relatif.*

— *Si b=1, cette équation à des solutions* $\iff$ $\overline{a}$ *est inversible dans* $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ $\iff$ a *est premier avec* n.
Dans ce cas, l'ensemble des solutions est $x_0 + kn$, *où* x_0 *est une solution particulière de* $ax \equiv 1 \pmod{n}$

— *Si* b *est qcq et* $a \wedge n = 1$. *Alors* $u_0 = bx_0$ *est une solution particulière avec* x_0 *solution de* $ax \equiv 1 \pmod{n}$. *L'ensemble des solutions de* $ax \equiv b \pmod{n}$ *est alors* $\{u_0 + kn | k \in \mathbb{Z}\}$.

— *Le cas général : l'équation* $ax \equiv b \pmod{n}$ *admet des solutions* $\iff$ $\delta = a \wedge n | b$.
Dans ce cas, les solutions sont les entiers de la forme : $\dfrac{b}{\delta}x'_0 + k\dfrac{n}{\delta}$ *avec* $k \in \mathbb{Z}$ *et* x'_0 *une solution particulière de l'équation* $\dfrac{a}{\delta}x \equiv \dfrac{b}{\delta} \pmod{\dfrac{n}{\delta}}$

Exemple 39. Grâce au théorème chinois, on peut résoudre certains systèmes de congruence :
Le système :

$$\begin{cases} k \equiv 2 \pmod 4 \\ k \equiv 3 \pmod 5 \\ k \equiv 1 \pmod 9 \end{cases}$$

admet pour solution les entiers de la forme $838 + 180k$ pour $k \in \mathbb{Z}$.