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

Notations : • A désigne un anneau commutatif, unitaire et intègre
• $\forall a \in A$, aA désigne l'idéal principal engendré par a

I. Etude théorique :

1. Définitions préalables :

Def 1 : Diviseur, multiple : Soient $x, y \in A$. On dit que x divise y dans A (ou que y est un multiple de x dans A) si il existe $z \in A$ tel que : $y = zx$. On note : $x \mid y$

Remarques : • $x \mid y \iff yA \subset xA$
• L'élément z tel que $y = zx$ est unique si $x \neq 0$

Def 2 : Element irréductible : $a \in A$ est dit irréductible s'il vérifie :
(i) $a \notin A^\times$ (ii) Si $a = bc$ avec $b, c \in A$, alors $b \in A^\times$ ou $c \in A^\times$

Def 3 : Factorisation en irréductibles : Soit $a \in A$, $a \neq 0$.
On dit que a admet une factorisation en irréductibles si il existe $u \in A^\times$ et $p_1, \dots, p_n$ des irréductibles de A tels que : $a = u p_1 p_2 \cdots p_n$
Si $a = v q_1 \cdots q_s$ est une autre décomposition, alors : $n = s$ et il existe une permutation σ de $\{1, 2, \dots, n\}$ telle que, pour tout $i \in [\![1, n]\!]$, $p_i = u_i q_{\sigma(i)}$ avec $u_i \in A^\times$.
(On dit que la décomposition de a est essentiellement unique)

2. Anneaux factoriels

Def 4 : Un anneau factoriel est un anneau commutatif unitaire intègre dans lequel tout élément non-nul admet une factorisation en irréductibles.

Ex : $\mathbb{Z}[i]$ est un anneau factoriel, $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel.

Def 5 : Une partie $\mathcal{P}$ de A (un anneau factoriel) est appelée système de représentants des irréductibles si elle vérifie :
(i) Tout élément de $\mathcal{P}$ est irréductible
(ii) $\forall q$ irréductible de A, $\exists ! \, p \in \mathcal{P}$, $u \in A^\times$: $q = up$.

Def 6 : Soit A un anneau commutatif unitaire intègre et $\mathcal{P}$ un système de représentants des irréductibles de A. On dit que A est factoriel si à tout $a \in A \setminus \{0\}$ on peut associer un unique couple constitué d'un élément $u \in A^\times$ et d'une application $v(a) : \mathcal{P} \longrightarrow \mathbb{N}$, $p \longmapsto v_p(a)$ tels que : $a = u \prod_{p \in \mathcal{P}} p^{v_p(a)}$
Cette écriture est appelée la décomposition de a en éléments irréductibles (relativement à $\mathcal{P}$) et $v_p(a)$ est la valuation p-adique de a.

Def 7 : PGCD, PPCM : Soient $a, b \in A$, A factoriel.
• Un PGCD de a et b est un élément δ de A tel que : $\delta = \prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$
(on note : $\delta = \mathrm{pgcd}(a, b)$)
• Un PPCM de a et b est un élément μ de A tel que : $\mu = \prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$
(on note $\mu = \mathrm{ppcm}(a, b)$)

Rq : δ et μ dépendent du système de représentants $\mathcal{P}$ choisi.

Thm 1 : Soit $a = (a_i)_{i \in I}$ une famille d'éléments de A et $\delta, \mu \in A$.
(i) δ est un pgcd de la famille a si et ssi : $\forall i \in I$, $\delta \mid a_i$ et si tout diviseur commun aux a_i divise δ
(ii) δ est un ppcm de la famille a si et ssi $\forall i \in I$, $a_i \mid \mu$ et si tout multiple commun aux a_i est un multiple de μ.

Thm 2 : Soit A factoriel, toute famille d'éléments de A admet un pgcd et un ppcm.

3 - Anneaux principaux

Déf 8 : Un anneau A unitaire, commutatif intègre est dit *principal* si tout idéal de A est engendré par un élément

Thm 3 : Tout anneau principal est factoriel

Thm 4 : Soit A un anneau principal, soit $a = (a_i)_{i \in [\![1,n]\!]}$ une famille d'éléments de A.
(i) Les pgcd de a sont les générateurs de l'idéal $a_1 A + \dots + a_n A$
(ii) Les ppcm de a sont les générateurs de l'idéal : $\bigcap_{i \in [\![1,n]\!]} a_i A$.

II - Propriétés des pgcd et ppcm.

Notation : A désigne un anneau factoriel

Prop 1 : Soient $x, y, z \in A$, on a :
- $\text{pgcd}(x,y,z) = \text{pgcd}(\text{pgcd}(x,y), z)$
- $\text{ppcm}(x,y,z) = \text{ppcm}(\text{ppcm}(x,y), z)$

Déf 9 : Soit $a = (a_i)_{i \in I}$ une famille d'éléments de A.
On dit que les a_i sont premiers entre eux si 1 est un pgcd de la famille a.

Thm 5 (Gauss) : Soient $a, b, c \in A$ tels que : $a \mid bc$ et $\text{pgcd}(a,b) = 1$
Alors $a \mid c$.

Notations : A désigne à présent un anneau principal.

Thm 6 : (Bezout) : Soient $a = (a_i)_{i \in [\![1,n]\!]}$ une famille d'éléments de A et δ un pgcd de a. Alors il existe $\lambda_1, \dots, \lambda_n \in A$ tels que :

$$\delta = \lambda_1 a_1 + \lambda_2 a_2 + \dots + \lambda_n a_n .$$

Thm 7 : Soient $a, b \in A$, on a : $ab\,A = (\text{ppcm}(a,b)\ \text{pgcd}(a,b))\,A$

III - Calculs effectifs de pgcd.

1 - Anneau euclidien

Déf 10 : L'anneau A (commutatif, unitaire, intègre) est dit *euclidien* s'il existe une application $\nu : A \setminus \{0\} \longrightarrow \mathbb{N}$ (appelée stathme euclidien) telle que :
(i) $\forall x, y \in A \setminus \{0\},\ x \mid y \Rightarrow \nu(x) \leqslant \nu(y)$
(ii) Si $a, b \in A \setminus \{0\}$, $\exists\, q, r \in A$ tels que $a = bq + r$ avec $r = 0$ ou $\nu(r) < \nu(b)$

Exemples : . $\mathbb{Z}$ muni du stathme $|\cdot|$ est euclidien
. $\mathbb{K}[X]$ (où $\mathbb{K}$ est un corps) muni du stathme $P \mapsto \deg P$ est euclidien.

Thm 8 : Tout anneau euclidien est principal

2 - Algorithmes de calcul du pgcd

Notations : A désigne un anneau euclidien

2.1 - Algorithme d'Euclide :

Entrées : $a, b \in A$
Sortie : un pgcd de a et b.

0) $r_0 \leftarrow a$ $\quad r_1 \leftarrow b$ $\quad i \leftarrow 1$
1) Tant que $r_i \neq 0$:
r_{i+1} donné par la division euclidienne $\begin{cases} r_{i-1} = r_i\, q_{i+1} + r_{i+1} \\ \nu(r_{i+1}) < \nu(r_i) \end{cases}$
$i \leftarrow i+1$
2) Renvoyer r_{i-1}

Complexité de l'algorithme dans $\mathbb{Z}$:

Thm 9 : Soit $n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$ tels que $a > b$ et tels que l'algorithme d'Euclide appliqué à a et b nécessite exactement n divisions. Supposons de plus que a soit minimal pour cette propriété. Alors $a = F_{n+1}$ et $b = F_n$ où (F_n) est la suite de Fibonacci définie par $F_0 = 0$, $F_1 = 1$ et $F_{i+2} = F_{i+1} + F_i$ pour $i \geq 0$.

Thm 10 : Si a et b sont inférieurs à N, le coût du calcul de $pgcd(a,b)$ par l'algorithme d'Euclide est en $O((\log_2 N)^2 + 1)$

2.2. Algorithme d'Euclide étendu

Entrées : $a, b \in A$

Sorties : $pgcd(a,b)$ et $u, v \in A$ tels que : $au + bv = pgcd(a,b)$

0) $r_0 \leftarrow a$; $r_1 \leftarrow b$; $i \leftarrow 1$; $U_1 = I_2$

1) Tant que $r_i \neq 0$

- $U_{i+1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} U_i$; $r_{i+1} \leftarrow r_{i-1} - q_{i+1} r_i$ (avec $v(r_{i+1}) < v(r_i)$)
- $i \leftarrow i+1$

2) Renvoyer r_{i-1}, $(U_i)_{1,1}$, $(U_i)_{1,2}$

Complexité de l'algorithme : identique à celle du précédent.

IV - Applications

Prop 1 : Soit $n \in \mathbb{N}$, $n \geq 2$ et soit $k \in \mathbb{Z}$.

$\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $pgcd(k,n) = 1$.

Prop 2 : Equation diophantienne du premier degré :

Soit A un anneau principal, $a, b, c \in A$. L'équation $ax + by = c$ possède des solutions dans A si et ssi $pgcd(a,b) \mid c$.

Thm 11 : Soient A un anneau principal, $a_1, \dots, a_m \in A$ tels que : $\forall i \neq j$, $pgcd(a_i, a_j) = 1$, et $a = \prod_{i=1}^{m} a_i$

Soient $\rho_i : A \to A/a_i A$ la surjection canonique et $\rho : A \to \prod_{i=1}^{m} A/a_i A$, $a \mapsto (\rho_1(a), \dots, \rho_m(a))$

Alors ρ induit un isomorphisme $\bar{\rho} : A/aA \to \prod_{i=1}^{m} A/a_i A$

Théorème 12 : Lemme des noyaux : Soit E un espace vectoriel sur un corps commutatif $\mathbb{K}$; soit $f \in \mathcal{L}(E)$ et $k \in \mathbb{N}^*$

Soient $P_1, \dots, P_k \in \mathbb{K}[X]$ premiers deux-à-deux et $P = \prod_{i=1}^{k} P_i$

Alors : $\operatorname{Ker} P(f) = \bigoplus_{i=1}^{k} \operatorname{Ker} P_i(f)$

Thm 13 (Théorème de Sophie Germain) : Soit p un nombre premier de Sophie Germain, ie un nombre premier impair tel que : $q = 2p+1$ soit premier.

Alors, il n'existe pas de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 [p]$ et $x^p + y^p + z^p = 0$.

Développement : Thm 13.

Bibliographie : Tauvel - Cours d'Algèbre

Fresnel - Anneaux

Nadière - Leçons d'Algèbre

Francinou, Gianella, Nicolas - Oraux X-ENS

Théorème de Sophie Germain : Soit p un nombre premier de Sophie Germain, ie : p impair et $q = 2p+1$ est premier

Alors il n'existe pas de triplet $(x,y,z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \ [p]$ et $x^p + y^p + z^p = 0$.

Dém : On raisonne par l'absurde : on suppose donné un triplet $(x,y,z) \in \mathbb{Z}^3$ tel que : $xyz \not\equiv 0 \ [p]$ et $x^p + y^p + z^p = 0$.

① Soit $d = pgcd(x,y,z)$. Posons $x' = \frac{x}{d}$, $y' = \frac{y}{d}$ et $z' = \frac{z}{d}$

Alors $pgcd(x',y',z') = 1$ et $x'^p + y'^p + z'^p = 0$ et $x'y'z' \not\equiv 0 \ [p]$

On suppose donc $pgcd(x,y,z) = 1$

• Supposons $pgcd(x,y) > 1$, soit p_0 un diviseur premier de ce pgcd.

Alors : $p_0 \mid x^p + y^p$, donc $p_0 \mid z^p = -(x^p + y^p) \Rightarrow p_0 \mid z$, absurde.

Donc x, y et z sont premiers entre eux deux à deux.

② Lemme 1 : $\exists (a,\alpha) \in \mathbb{Z}$: $x + y = a^p$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$

Preuve : On a : $(y+z) \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = y^p + z^p = -x^p = (-x)^p \Rightarrow \alpha = -x$.

Montrons par l'absurde que $(y+z)$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux.

Soit p_0 un diviseur premier commun.

$p_0^2 \mid -x^p \Rightarrow p_0 \mid x$

De plus : $p_0 \mid y+z \Rightarrow y \equiv -z \ [p_0]$

D'où : $\sum_{k=1}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=1}^{p-1} y^{p-1} \equiv p\, y^{p-1} \equiv 0 \ [p_0]$

$\Rightarrow p_0 \mid p\, y^{p-1} \underset{\text{Gauss}}{\Rightarrow}$ ① $p_0 \mid p \Rightarrow p_0 = p \Rightarrow p \mid x$ $\Rightarrow$ absurde par hypothèse

② $p_0 \mid y^{p-1} \Rightarrow p_0 \mid y \Rightarrow x$ et y ne sont pas premiers entre eux, absurde.

$\Rightarrow (y+z)$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux

$\Rightarrow (y+z) \sum_{k=0}^{p-1} (-z)^{p-1-k} = \alpha^p \Rightarrow \exists a : y+z = a^p$ (Thm admis : $a \wedge b = 1$ et $ab = c^k$ $\Rightarrow a = \alpha^k$ et $b = \beta^k$)

Par symétrie : $\exists (b,c) \in \mathbb{Z}^2$: $x+z = b^p$ et $x+y = c^p$

③ Lemme 2 : $m \in \mathbb{Z}$, $q \nmid m$. Alors : $m^p \equiv \pm 1 \ [q]$

Dem : $q \nmid m \Rightarrow$ (PTF) : $m^{q-1} \equiv 1 \ [q] \Rightarrow m^{2p} \equiv 1 \ [q]$

Comme $\mathbb{Z}/q\mathbb{Z}$ est un corps, $m^p \equiv \pm 1 \ [q]$

④ Montrons qu'un des entiers x, y ou z est divisible par q, et qu'il est unique.

Par l'absurde, supposons qu'aucun n'est divisible par q.

On a : $x^p \equiv \pm 1 \ [q]$, $y^p \equiv \pm 1 \ [q]$, $z^p \equiv \pm 1 \ [q]$

Ainsi : $x^p + y^p + z^p \equiv \begin{cases} \pm 1 \\ \text{ou} \\ \pm 3 \end{cases} [q]$, ce qui est absurde.

Donc un des trois entiers est divisible par q. Il est unique car x, y et z sont premiers entre eux.

Dans la suite, on suppose $q \mid x$, ainsi : $yz \not\equiv 0 \ [q]$.

⑤ On a : $\begin{cases} x + y = c^p \\ x + z = b^p \\ y + z = a^p \end{cases} \Rightarrow 2x = b^p + c^p - a^p \equiv 0 \ [q]$

Ainsi : $y \equiv c^p \ [q]$. On $q \nmid y \Rightarrow q \nmid c$, $y \equiv \pm 1 \ [q]$

De même : $z \equiv \pm 1 \ [q]$

De plus, $q \mid a$ (conséquence du Lemme 2)

D'où : $y + z \equiv 0 \ [q]$

D'après le lemme 1 : $\alpha^p \equiv p\, y^{p-1} \ [q]$.

$\Rightarrow \alpha^p \equiv p\,(\pm 1)^{p-1} \ [q]$

$\equiv p \ [q]$ car $p-1$ pair.

Absurde car $\alpha^p \equiv \begin{cases} -1 \\ 0 \\ 1 \end{cases} [q]$ d'après le lemme 2.

Donc il ne peut exister de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0 \ [p]$ et $x^p + y^p + z^p = 0$.