142 PGCD et PPCM, algorithmes de calcul. Applications.

I PGCD et PPCM dans un anneau factoriel

A Généralités [PER]

DÉFINITION 1 : [GROUPE DES INVERSIBLES]
On pose $A^* = \{a \in A | b \in A, ab = 1\}$ le groupe des inversibles de A, aussi appelés "unités de A".

EXEMPLE 2 : Si A est un corps, alors $A^* = A\backslash\{0\}$

DÉFINITION 3 : [DIVISIBILITÉ]
Soient $a, b \in A$. On dit que a divise b et on écrit $a|b$ si et seulement si il existe $c \in A$ tel que $b = ac$.

PROPOSITION 4
On a : $b|a$ si et seulement si $(a) \subset (b)$.

DÉFINITION 5 : [ÉLÉMENTS ASSOCIÉS]
Soient $a, b \in A$. On dit que a et b sont associés si $a|b$ et $b|a$ (ou s'il existe $u \in A^*, a = bu$)

REMARQUE 6
C'est une relation d'équivalence. Les éléments associés jouent des rôles identiques pour la divisibilité.

DÉFINITION 7 : [IRRÉDUCTIBLE]
Soient $p \in A$. On dit que p est irréductible si et seulement si on a :
i) $p \notin A^*$
ii) Si $p = ab$ alors $a \in A^*$ ou $b \in A^*$.

EXEMPLE 8 : Dans $\mathbb{Z}$ les irréductibles sont les nombres premiers.

DÉFINITION 9 : [ANNEAU FACTORIEL]
Soit A un anneau. On dit que A est factoriel si :
i) A est intègre,
ii) Tout élément a on nul de A s'écrit $a = up_1...p_r$ avec $u \in A^*$ et $p_1, ..., p_r$ irréductibles
iii) Cette décomposition est unique, à permutation près et à des inversibles près : si $a = up_1...p_r = vq_1...q_s$ alors on a $r = s$ et il existe $\sigma \in S_r$ tel que p_i et $q_{\sigma(i)}$ soient associés.

EXEMPLE 10 : $\mathbb{Z}$ est factoriel.
Dans ce qui suit on suppose que A est factoriel.

DÉFINITION 11 : [PGCD, PPCM]
Soient $a, b \in A$ tels que $a = \prod p^{v_p(a)}$ et $b = \prod p^{v_p(b)}$ où v_p est la valuation p-adique.
i) On appelle plus petit multiple commun de a et b l'élément
$ppcm(a, b) = \prod p^{sup(v_p(a), v_p(b))}$
ii) On appelle plus grand commun diviseur de a et b l'élement
$pgcd(a, b) = \prod p^{inf(v_p(a), v_p(b))}$

REMARQUE 12
i) Le ppcm et le pgcd ne sont définis qu'aux éléments inversibles près.
ii) On définit par récurrence le pgcd et le ppcm de n éléments.

B Contenu d'un polynôme [PER] [GOU]

DÉFINITION 13 : [CONTENU]
Soit $P \in A[X]$ non nul, on appelle contenu de P, noté $c(P)$ le plus grand commun diviseur de ses coefficients. L'élément $c(P)$ est défini modulo A^*. Un polynôme P est dit primitif si on a $c(P) = 1$.

LEMME 14 : [LEMME DE GAUSS]
On a $c(PQ) = c(P)c(Q)$ modulo A^*.

THÉORÈME 15 : [THÉORÈME DE GAUSS]
Si A est factoriel, $A[X]$ est factoriel.

DÉVELOPPEMENT : [CRITÈRE D'EISENSTEIN] [GOU p62]
Soit A un anneau factoriel. On note $K = Frac(A)$.
Soit $n \in \mathbb{N}^*$ et $P = a_nX^n + ... + a_1X + a_0 \in A[X]$. On suppose qu'il existe p irréductible dans A tel que $p \not| a_n, p^2 \not| a_0$ et $p|a_i$ pour tout $i \in [\![0, n-1]\!]$.
Alors P est irréductible dans $K[X]$.

APPLICATION 16 : Soit p premier dans $\mathbb{Z}$. Alors $\phi(X) = X^{p-1} + ... + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

C Cas des anneaux principaux [PER]

DÉFINITION 17 : [ANNEAU PRINCIPAL]
Un anneau A est dit principal s'il est intègre et si tout idéal de A est principal.

EXEMPLE 18 : $\mathbb{Z}$ est principal.

PROPOSITION 19
Un anneau principal est factoriel.

THÉORÈME 20 : [THÉORÈME DE BÉZOUT]
Soit A un anneau principal, soient $a, b \in A\backslash\{0\}$ et soit $d = pgcd(a, b)$. Alors on a $(d) = (a) + (b)$ ou encore il existe $\lambda, \mu \in A$ tels que $d = \lambda a + \mu b$.

COROLLAIRE 21
Soit A un anneau principal, soient $a, b \in A\backslash\{0\}$ tels que $pgcd(a, b) = 1$.
Alors $(a) + (b) = (1)$ ie. il existe $\lambda, \mu \in A$ tels que $\lambda a + \mu b = 1$.

REMARQUE 22
Le théorème de Bézout est en défaut dans un anneau factoriel non principal. Ainsi l'anneau $k[X, Y]$ est factoriel et X et Y sont premiers entre eux mais on a $(X) + (Y) = (X, Y) \neq (1)$.

II Algorithmes de calcul dans un anneau euclidien

A Obtention du PGCD [PER] [PIC]

DÉFINITION 23 : [ANNEAU EUCLIDIEN]
Un anneau est dit euclidien si :
i) A est intègre,
ii) A est muni d'une division euclidienne, ie. il existe une fonction (appelée parfois stathme) $v : A\backslash\{0\} \to \mathbb{N}$ telle que si $a, b \in A\backslash\{0\}$, il existe $q, r \in A$ avec $a = bq + r$ et ($r = 0$ ou $v(r) < v(b)$)

PROPOSITION 24
Un anneau euclidien est principal.

EXEMPLE 25 : L'anneau $\mathbb{Z}$ muni de l'application $v(n) = |n|$ est euclidien.

LEMME 26 : [DIVISION EUCLIDIENNE DANS A[X]]
Soit A un anneau et soit $P \in A[X]$, $P \neq 0$, de coefficient dominant inversible.
Soit $F \in A[X]$, il existe $Q, R \in A[X]$, tels que l'on ait :
i) $F = PQ + R$,
ii) $dR < dP$ ou $R = 0$

CORROLAIRE 27
Si k est un corps, l'anneau $k[X]$ est euclidien (avec pour stathme $v(P) = dP$).

EXEMPLE 28 : L'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est principal mais n'est pas euclidien.

ALGORITHME D'EUCLIDE
On utilise la division euclidienne en s'appuyant sur le fait que si $a = bq + r$ avec $r \neq 0$ alors $pgcd(a, b) = pgcd(b, r)$ [VOIR ANNEXE]

EXEMPLE 29 : Pour déterminer le PGCD de 50 et 9 :
i) $50 = 9 \times 5 + 5$,
ii) $9 = 5 \times 1 + 4$,
iii) $5 = 4 \times 1 + 1$
D'où $pgcd(50, 9) = 1$.

PROPOSITION 30 : [COMPLEXITÉ]
Le calcul du $pgcd$ de a et de b par l'algorithme d'Euclide a une complexité de $O(loga \times logb)$ opérations binaires dans le pire des cas.

B Obtention d'une relation de Bézout [PIC]

ALGORITHME D'EUCLIDE ÉTENDU
En remontant dans l'algorithme d'Euclide, on obtient une relation de Bézout.

EXEMPLE 31 : La division euclidienne de $x^2 + 3x + 4$ par $x + 1$ est :
i) $x^2 + 3x + 4 = (x + 1)(x + 2) + 1$,
ii) On en déduit une relation de Bézout $x^2 + 3x + 4 - (x + 2)(x + 1) = 1$

III Applications

A Équations diophantiennes [ROM] [FRA]

DÉFINITION 32 : [ÉQUATION DIOPHANTIENNE]
Une équation diophantienne est une équation polynômiale à coefficients entiers et à inconnues entières.

EXEMPLE 33 : Soit $n \geq 2$, $a \in N\backslash\{0\}$, $b \in \mathbb{Z}$, alors $ax \equiv b[n]$ est une équation diophantienne.

PROPOSITION 34
L'équation $ax \equiv 1[n]$ a des solutions si et seulement si $\bar{a} \in \mathbb{Z}_n^*$ si et seulement si $pgcd(a,n) = 1$.

COROLAIRE 35
Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}\backslash\{0\}$ tels que $pgcd(a,n) = 1$. Alors l'ensemble des solutions de $ax \equiv 1[n]$ est :
$S = \{x_0 + kn | k \in \mathbb{Z}\}$ avec x_0 une solution particulière.

THÉORÈME 36
L'équation diophantienne $ax \equiv b[n]$ pour $a \in \mathbb{N}\backslash\{0\}$, $b \in \mathbb{Z}$ et $n \geq 2$ a des solutions entières si et seulement si $pgcd(a,n)|b$. Dans ce cas, l'ensemble des solutions de cette équation est l'ensemble $S = \{b'x_0' + kn' | k \in \mathbb{Z}\}$ où x_0' est une solution particulière de $a'x \equiv 1[n']$ où $a = a'.pgcd(a,n)$ et $n = n'.pgcd(a,n)$.

REMARQUE 37
On peut généraliser à $\sum a_i x_i = b$ par récurrence.

DÉVELOPPEMENT : [THÉORÈME DE SOPHIE - GERMAIN] [FRA p167]
Soit p 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 $p \not| xyz$ et $x^p + y^p + z^p = 0$

B Systèmes de congruence [ROM]

THÉORÈME 38 [THÉORÈME DES RESTES CHINOIS]
Soit $(n_j)_{1\leq j\leq r}$ une suite de $r \geq 2$ entiers naturels distincts de 0 et 1 et $n = n_1...n_r$.
Les entiers $n_1, ..., n_r$ sont deux à deux premiers entre eux si et seulement si les anneaux $\mathbb{Z}_n$ et $\mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r}$ sont isomorphes. Dans ce cas l'application :

$$\begin{array}{rccc} \psi : & \mathbb{Z}_n & \to & \mathbb{Z}_{n_1} \times ... \times \mathbb{Z}_{n_r} \\ & \pi_n(k) & \mapsto & (\pi_1(k), ..., \pi_r(k)) \end{array}$$

(où on a noté π_k la surjection canonique π_{n_k}) est un isomorphisme d'anneaux d'inverse :

$$\begin{array}{rccc} \psi^{-1} : & Z_{n_1} \times ... \times \mathbb{Z}_{n_r} & \to & \mathbb{Z}_n \\ & (\pi_1(a_1), ..., \pi_r(a_r)) & \mapsto & \pi_n(\sum a_i u_i \frac{n}{n_i}) \end{array}$$

où $(u_j)_{1\leq j\leq r}$ est une suite d'entiers relatifs telle que $\sum_{j=1}^r u_j \frac{n}{n_j} = 1$.

EXEMPLE 39 : $\mathbb{Z}_4$ n'est pas isomorphe à $\mathbb{Z}_2 \times \mathbb{Z}_2$.

EXEMPLE 40 : L'ensemble des solutions du système d'équations diophantiennes

$$\begin{array}{l} k \equiv 2[4] \\ k \equiv 3[5] \\ k \equiv 1[9] \end{array}$$

est $S = \{118 + 180k | k \in \mathbb{Z}\}$

Références :

[PER] Cours d'Algèbre Daniel Perrin Ellipses

[ROM] Mathématiques pour l'agrégation : Algèbre et géométrie Jean-Etienne Rombaldi

[FRA] S. FRANCINOU, H. GIANELLA et S. NICOLAS : Oraux X-ENS - Algèbre 1. Cassini, 2007

[PIC] Saux Picart, cours de calcul formel : algorithmes fondamentaux